LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°35 — octobre 2021

Parution trimestrielle
Gratuite

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

La transparence des sociétés, trusts et autres constructions juridiques : le serpent de mer de la lutte contre le blanchiment

À la suite de la révélation de plusieurs cas de blanchiment mettant en cause des établissements financiers au sein de l'Union européenne, le Conseil de l'Union européenne a demandé à la Commission de procéder à « une analyse rétrospective » de ces cas de blanchiment[1] allégués. Le rapport[2] portant sur un échantillon de dix banques[3] au cours de la période 2012-2018 met en évidence des lacunes et de nombreuses défaillances. Outre des difficultés rencontrées par de nombreux établissements pour identifier des bénéficiaires effectifs se cachant derrière leurs clients, certains n'hésitaient pas à accepter comme clients, des entités commerciales, dont le bénéficiaire effectif ne pouvait être identifié.

L'identification du bénéficiaire effectif est la pierre d'achoppement de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) mais aussi un véritable serpent de mer qui surgit chaque fois qu'un nouveau scandale éclate. Le dernier en date des « Pandora papers » n'échappe pas à la règle.

L'onde de choc passée, rien ne change, jamais.

L'utilisation de sociétés-écrans, offshore, trusts et autres constructions juridiques empilées dans des montages complexes à des fins de blanchiment de capitaux et de financement du terrorisme a été identifiée de longue date par le Groupe d'action financière (GAFI), dès sa création en 1989.

Ces instruments juridiques sont mis à la disposition de quiconque, par des officines qui les vendent clés en main, y compris au sein même de l'Union européenne et qui ne servent qu'à contourner toute forme de régulation en permettant à leurs propriétaires réels de se cacher derrière des masques, des actionnaires et dirigeants prête-noms.

SOMMAIRE

ÉDITO 1

INTERVIEW

SOPHIE HATT, DIRECTRICE DE LA COOPÉRATION INTERNATIONALE DE SÉCURITÉ (DCIS) 4

CONSTATS ET PRÉCONISATIONS

LA LUTTE CONTRE LE TERRORISME ET LA CRIMINALITÉ ORGANISÉE EN MATIÈRE DE RENSEIGNEMENT
PAR PAULINE BONNECARRÈRE 9

PHÉNOMÉNOLOGIE DE LA CRIMINALITÉ ORGANISÉE

COURTIERS DU CRIME
PAR QUENTIN MUGG 18

DOCTRINE

ÉTAT CIVIL, IDENTITÉ ET BIOMÉTRIE, EN PRATIQUE, QU'EST- CE QUE L'IDENTITÉ LÉGALE ?
PAR MARIANNE BONDAZ 24

COMPLIANCE / CONFORMITÉ

LA LOI SAPIN II À L'ÉPREUVE DE L'INTERNATIONAL
PAR VÉRONIQUE BRUNEAU BAYARD 31

GOUVERNANCE ET ANTICORRUPTION
PAR NATHALIE KALESKI 37

BANQUES SUISSES ET RÈGLES ANTI-BLANCHIMENT
PAR CARLO LOMBARDINI 41

REGARDONS AILLEURS

LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN AMÉRIQUE LATINE : LES DÉFIS DE LA COOPÉRATION
PAR XAVIER COUSQUER 47

LA CORRUPTION EN AFRIQUE
PAR IHSANE EL HASSANI 54

Le GAFI et la Commission européenne ont cru trouver le Graal en imposant aux entités assujetties aux dispositifs LBC-FT d'identifier le bénéficiaire effectif défini comme la ou les personnes physiques qui, en dernier ressort, possèdent ou contrôlent une entité juridique, un trust exprès ou une construction juridique similaire ou/et la personne physique pour le compte ou au bénéfice de laquelle une transaction est exécutée ou une activité réalisée. En théorie il s'agit bien d'une obligation de résultat qui, si elle n'est pas satisfaite devrait conduire les assujettis à faire une déclaration d'opération suspecte auprès de la cellule de renseignement financier.

Mais en pratique, les choses ne vont pas ainsi en raison de la possibilité, laissée intacte par le nouveau paquet législatif européen de lutte contre le blanchiment et le financement du terrorisme[4], de recourir à des actionnaires et dirigeants prête-noms.

Certes, le nouveau dispositif prévoit que ces prête-noms devront conserver des informations adéquates, exactes et actuelles sur l'identité de leur mandant, ainsi que sur le ou les bénéficiaires effectifs de celui-ci et déclarer ces informations ainsi que leurs statuts aux sociétés ou autres entités juridiques. Certes, les sociétés auront à leur tour, l'obligation de consigner ces informations dans des registres mis en place conformément à l'article 10 de la future sixième directive et déclarer ces informations aux entités assujetties lorsque celles-ci prennent des mesures de vigilance à l'égard de la clientèle.

Mais croit-on sérieusement venir à bout des effets criminogènes de ces entités de cette manière ?

En réalité, depuis le début, les organisations internationales et la Commission font fausse route en imposant une obligation d'identifier le bénéficiaire effectif. Il serait bien plus efficace d'imposer à l'échelle de l'Union européenne la transparence de la propriété du capital des sociétés et des constructions juridiques dès leur création de manière à neutraliser juridiquement ces entités, que d'aucunes prétendent utiles à des activités licites, alors même que leurs promoteurs ne parviennent pas à expliquer quelle pourrait être leur utilité licite et en quoi elles sont utiles à l'économie réelle.

En réalité, tant qu'il sera possible de constituer des masques juridiques derrière lesquels se cachent les membres des organisations criminelles, les potentats qui spolient leurs peuples et les fraudeurs en tous genres, l'expansion de l'économie criminelle s'étendra jusqu'à faire disparaître nos démocraties.

Notes :

1. https://www.consilium.europa.eu/media/37283/st15164-en18.pdf
2. COM(2019)373 final Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des récents cas présumés de blanchiment de capitaux impliquant es établissements de crédit de l'Union européenne.
3. « ABLV Bank en ce qui concerne les événements qui ont conduit à la fermeture de la banque, Danske Bank en ce qui concerne les événements qui ont conduit à la fermeture de sa succursale estonienne, Deutsche Bank en ce qui concerne l'affaire des transactions miroirs qui a conduit à l'imposition d'amendes, FBME Bank en ce qui concerne les événements qui ont conduit à sa fermeture, ING en ce qui concerne les événements qui ont provoqué l'arrangement avec le ministère public des Pays-Bas, Nordea en ce qui concerne les événements qui ont donné lieu à des amendes pour manque de conformité aux règles en matière de lutte contre le blanchiment de capitaux, Pilatus Bank en ce qui concerne les événements qui ont conduit à sa fermeture, Satabank en ce qui concerne les événements qui ont conduit à des restrictions de ses activités, Société Générale en ce qui concerne les événements qui ont conduit à l'imposition d'amendes pour manque de conformité aux règles en matière de lutte contre le blanchiment de capitaux et Versobank en ce qui concerne les événements qui ont mené à la fermeture de la banque ».
4. Règlement du Parlement européen et du Conseil instituant l'Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme et modifiant les règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010 Règlement du Parlement européen et du Conseil relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, COM(2021) 420 final ci-après Directive du Parlement européen et du Conseil relative aux mécanismes à mettre en place par les États membres pour prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et abrogeant la directive (UE) 2015/849, modifiée par la directive (UE)2018/843 et Règlement COM (2021)422 final qui procède à la refonte du règlement (UE) 2015/847.

COMITÉ SCIENTIFIQUE DE LA REVUE DU GRASCO

FALLETTI François

Ancien magistrat, il a exercé plus de 15 ans au sein de la Direction des affaires criminelles et des Grâces du ministère de la Justice dont il a été le directeur de 1993 à 1996. Il a ensuite été procureur général près les cours d'appel de Lyon, Aix en Provence et Paris. Avocat général à la cour de cassation, il a été le membre français de l'Unité Eurojust à La Haye (2004-2008). Il a également exercé les fonctions de président de l'association internationale des procureurs (2007-2010), de secrétaire général de l'association internationale des procureurs francophones (2009-2018), et assuré la mission de conseiller spécial auprès de Madame le Commissaire européen pour la Justice (2016-2017). Docteur en droit, diplômé de Sciences-po Paris, il est l'auteur de plusieurs ouvrages, notamment du "précis de droit pénal et de procédure pénale" (PUF 7e édition 2018) coécrit avec Frédéric Debove. Il est aujourd'hui avocat au Barreau de Lyon.

LABORDE Jean-Paul

Conseiller honoraire à la Cour de cassation et ancien Directeur exécutif du comité des Nations Unies chargé de la lutte contre le terrorisme avec rang de Sous-Secrétaire général. Il est actuellement ambassadeur itinérant de l'Assemblée parlementaire de la Méditerranée, Directeur du Centre d'expertise sur la lutte contre le terrorisme, titulaire de la Chaire Cyber à l'École de St-Cyr Coëtquidan et Conseiller spécial de l'Initiative mondiale de lutte contre le crime transnational organisé.

LEBLOIS-HAPPE Jocelyne

Professeur à L'Université de Strasbourg et chargée de cours à l'Université Albert-Ludwig de Fribourg-en-Brisgau (Allemagne). Elle est membre du groupe European Criminal Policy initiative.

MATHON Claude

Avocat général honoraire à la Cour de cassation (chambre criminelle). Après avoir Développé une carrière essentiellement comme procureur de la République, il a dirigé le Service Central de prévention de la Corruption (2001). Spécialisé en intelligence économique, il a présidé à la rédaction de trois rapports : « Entreprise et intelligence économique, quelle place pour la puissance publique ? - 2003 », « Intelligence économique et corruption - 2004 », « la protection du secret des affaires : enjeux et propositions-2009 ».

PRADEL Jean

Ancien magistrat (de 1959 à 1969), il obtient l'agrégation en droit privé et en sciences criminelles en 1969. D'abord affecté à la Faculté de droit de Tunis, il devient professeur à la Faculté de droit à Poitiers (1972). Depuis 2003, il est professeur émérite de l'Université de Poitiers. Il est directeur honoraire de l'institut de sciences criminelles de Poitiers. Il a présidé l'Association française de droit pénal. Il participe à de nombreux congrés internationaux. Il est l'auteur de nombreux ouvrages, notamment - Droit pénal général, Procédure pénale, Droit pénal comparé, Droit pénal spécial en collaboration avec M. Danti-Juan, Droit pénal européen avec G. Corsten et G. Vermeulen.

SORDINO Marie-Christine

Professeur à l'Université de Montpellier, Directrice de l'Équipe de droit pénal (EDPM-UMR 5815), Directrice du Master 2 Droit pénal fondamental et du Master 2 Pratiques pénales. Elle est auteur de nombreux ouvrages dont Mutations du droit pénal, entre affirmation de valeurs et protection des libertés ?, Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, décembre 2017 ; Lanceur d'alerte : innovation juridique ou symptôme social ?, Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, décembre 2016 ; Innovation numérique et droit pénal économique et financier : enjeux et perspectives, Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, mai 2016 . Elle est cotitulaire de la chronique « Sanctions » au Bulletin Joly des entreprises en difficulté (BJE), titulaire de la chronique « Droit de la concurrence », RSC et expert auprès d'organismes nationaux et internationaux.

STRICKLER Yves

Docteur de l'Université de Strasbourg, Maître de conférences à Toulouse, Professeur à Nancy, puis à Strasbourg, il exerce depuis 2010 à l'Université Côte d'Azur. Membre du Haut Conseil de la Magistrature de la Principauté de Monaco, il dirige à Nice l'Institut fédératif de recherche "interactions".

STORCK Michel

Professeur émérite à l'Université de Strasbourg.

INTERVIEW

SOPHIE HATT, DIRECTRICE DE LA COOPÉRATION INTERNATIONALE DE SÉCURITÉ (DCIS)

PROPOS RECUEILLIS PAR JOCELYNE KAN, RÉDACTRICE EN CHEF DE LA REVUE DU GRASCO

L.R.D.G. : Quelles sont les missions de la Direction de la coopération internationale de sécurité (DCIS) qui a été restructurée le 1er août 2021 ?

La direction de la coopération internationale de sécurité, DCIS, est une direction commune de la police et de la gendarmerie nationales. Elle est née le 1er août 2021 d'une réforme structurelle de la direction de la coopération internationale (DCI) dont l'organisation datait de sa création en 2010.

Les missions de la DCIS restent d'animer et de coordonner les coopérations opérationnelles, techniques et institutionnelles des directions générales de la police et de la gendarmerie nationales à l'étranger grâce à notre réseau de 73 services de sécurité intérieure (SSI) implantés dans les ambassades françaises, couvrant pas moins de 153 pays.

En coordination avec la nouvelle Direction des Affaires Européennes et Internationales (DAEI) rattachée au secrétariat général du

ministère de l'Intérieur, la DCIS participe à l'application de la stratégie internationale du ministère de l'Intérieur et à la mise en oeuvre de la politique étrangère de la France dans tous les domaines relevant du ministère de l'Intérieur, à l'exception des questions relevant exclusivement des services de renseignement. La DCIS participe activement à la présence française dans les institutions internationales que sont l'ONU et l'Union européenne, notamment en proposant des candidatures et en défendant les positions de notre gouvernement.

L'action des policiers et gendarmes de la DCIS vise un retour en sécurité intérieure en permettant de mieux contrer les menaces qui prennent naissance hors de nos frontières ; on pense naturellement à la criminalité transnationale organisée, les trafics de drogues et d'armes, la cybercriminalité, le terrorisme ou encore le trafic d'êtres humains. Chaque année, les thématiques prioritaires sont assignées par le ministre lui-même.

À l'approche de la présidence française de l'Union européenne, la DCIS s'est mise en ordre de marche pour contribuer à son succès, en portant et mettant en application les projets de l'État français.

L.R.D.G. : Comment la DCIS est-elle composée et organisée ?

Pour remplir ses missions, la DCIS est tout d'abord composée d'un échelon central implanté en région parisienne qui est constitué de 259 policiers, gendarmes et personnels administratifs. Ensuite, la direction

dispose d'un réseau de 73 SSI qui regroupe 286 policiers et gendarmes, placés sous l'autorité des attachés de sécurité intérieure (ASI). Ce réseau, il faut le savoir, répond à une logique d'agilité, puisqu'en fonction de l'évolution de la situation dans les pays et des priorités ministérielles, nous sommes en capacité permanente de le faire évoluer.

À la centrale, la direction comporte un état-major qui est l'unique point d'entrée des informations opérationnelles en provenance du réseau et des requêtes des services de la police et de la gendarmerie nationales. Il y a également une sous-direction Monde, une sous-direction Europe et une sous-direction administration et soutien, cette dernière assurant la gestion des ressources humaines.

La sous-direction Europe a pour rôle d'animer et coordonner la coopération institutionnelle et technique des pays membres de l'Union européenne et de son voisinage. Elle intervient à différents niveaux sur l'ensemble des grands sujets européens de sécurité intérieure et de coopération en liaison avec les directions générales de la police et de la gendarmerie nationales. Les axes de travail sont multiples et comprennent l'animation de la coopération institutionnelle, la coopération technique bilatérale avec les pays de l'UE et des Balkans, l'influence et le placement des policiers et gendarmes auprès des missions internationales, l'animation du réseau des experts nationaux détachés, la réalisation de projets de coopération et financements européens ou encore l'activité du Fonds pour la sécurité intérieure.

La sous-direction Monde, quant à elle, conçoit et met en oeuvre la coopération technique sur les autres régions du globe, dont certaines sont particulièrement vulnérables et constituent de fortes priorités pour notre ministère comme l'Afrique qui bénéficie d'une action appuyée sur la zone sahélienne, le Maghreb, le Moyen-Orient et Proche-Orient et l'Europe orientale. L'animation des réseaux d'influence de la DCIS (réseau de formation francophone Francopol et Résopolis), le partenariat avec les entreprises de la filière sécurité ainsi que les formations académiques en France au profit des stagiaires étrangers y sont également regroupés.

Enfin, une plateforme H24 assure une assistance opérationnelle à notre réseau des SSI et, par leur intermédiaire, participe à l'échange permanent d'informations entre nos services de police et gendarmerie français et ceux de l'étranger.

L.R.D.G. : Quelles sont les relations de la DCIS avec le secteur privé dans le cadre de la mise en oeuvre de la diplomatie économique ?

La DCIS encourage la promotion de nos entreprises nationales et de nos technologies sur le terrain. Il s'agit d'accompagner celles qui le souhaitent en leur montrant les possibilités des marchés en développement au sein des pays qui accueillent notre réseau de SSI. Au-delà des informations fournies, le ministère est en mesure de renseigner nos entreprises nationales sur les marchés publics et d'assurer la liaison entre elles et le réseau du ministère. C'est pourquoi, depuis 2010, un bureau est dédié aux partenariats, qui a pour mission principale le soutien à l'exportation des équipements proposés par des entreprises françaises de la filière sécurité, et qui est également désigné comme le point d'entrée des directions sûreté des groupes industriels français pour leur prodiguer des conseils ou leur prêter assistance, en lien avec nos ASI en poste.

Les équipements en question peuvent être des équipements de protection individuelle et collective, du matériel d'identification et d'appui à l'enquête judiciaire, de la sécurisation des sites… En revanche, je me dois de souligner que ce rôle de facilitateur exclut toute forme de participation commerciale. Il s'inscrit dans la droite ligne de la diplomatie économique et le respect des règles de la concurrence. En effet, le bureau des partenariats agit en fonction des orientations et prescriptions définies au niveau politique et ne s'implique jamais dans les aspects purement commerciaux. Son action s'exerce dans le respect d'une charte éthique qui lui impose la transparence et l'impartialité dans les sollicitations qui lui sont adressées.

Par ailleurs, c'est un acteur majeur de l'organisation d'événements tels que MILIPOL ou encore le Forum international de la Cyber-sécurité (FIC). La DCIS accompagne les délégations étrangères dans ces salons afin de valoriser auprès d'elles les compétences françaises.

L.R.D.G. : Comment sont menées les actions de coopération dans les pays pour lutter notamment contre le terrorisme, la criminalité organisée transnationale, la cybercriminalité, les escroqueries (faux ordre de virement international, fraude au président) dont sont victimes des personnes morales et physiques ?

Les SSI remplissent des missions variées allant de la coopération

technique (actions de formations, missions d'experts, renforcement des capacités des forces de sécurité intérieures locales) à la coopération institutionnelle en passant par la coopération opérationnelle. Ces différents types de coopération ont pour vocation de favoriser un retour en sécurité intérieure. En effet, l'analyse des phénomènes criminels dans les pays où la DCIS est implantée permet d'anticiper ceux susceptibles d'impacter notre pays. Dès lors, une réponse opératonnelle peut être préparée en amont de leur survenance, notamment en partageant l'information avec les services d'investigation et/ou de renseignement concernés. La lutte contre les trafics de stupéfiants en est le parfait exemple. En coordination avec l'OFAST (office anti-stupéfiants), il est nécessaire d'identifier les containers susceptibles de contenir de la drogue en partance d'Amérique du sud et à destination de l'Europe. Cela permet d'intercepter les containers ou d'identifier les personnes chargées de les récupérer à l'arrivée, en vue de leur interpellation. Nos services au Brésil ou en République dominicaine sont à la pointe de ces actions, sachant que les SSI implantés dans les pays producteurs, ou connus comme servant de base pour les organisateurs de ces trafics, fournissent une masse d'informations importantes que nous partageons. En Colombie, notre SSI échange parfaitement avec les autorités policières locales en matière de renseignement et leur apporte un soutien actif. En 2020, cette coopération a permis la saisie d'une tonne de cocaïne, 3 tonnes de précurseurs chimiques, des véhicules et des armes ainsi que le démantèlement complet d'une organisation criminelle.

La force de notre réseau réside dans cette proximité qu'il met en place avec les autorités des pays de leur zone de compétence. Ces relations de confiance permettent d'accélérer les actions policières ou judiciaires. Par exemple, les escroqueries par faux ordre de virement au préjudice des entreprises françaises nécessitent une réponse quasi immédiate afin de bloquer les fonds détournés. Le travail de nos postes en Hongrie et en Pologne a permis la restitution de 4,8 millions d'euros aux victimes et le second de 1,5 millions d'euros. Notre action s'inscrit en appui d'une démarche judiciaire.

Pour autant, la DCIS n'a pas vocation à se substituer aux canaux institutionnels que sont EUROPOL et INTERPOL. Notre réseau vient compléter ces dispositifs multilatéraux, dans l'intérêt des services français, en permettant un suivi dans le pays et une remontée d'information optimale pour la délinquance du haut du spectre. À ce titre, la lutte contre le terrorisme, contre les trafics d'êtres humains et contre la criminalité organisée transnationale font partie de nos priorités. Pour cela, la DCIS et la DCPJ (direction centrale de la police judicaire) entretiennent des échanges d'une grande qualité.

L'implication française dans la lutte contre la traite des êtres humains et les filières d'immigration clandestine, notamment au Niger, permet d'identifier et de faire démanteler des filières par les autorités locales, avant même que les migrants n'arrivent aux portes de l'Europe. Tous les SSI contribuent, par leurs analyses, à mieux comprendre ce phénomène, permettant ainsi une réponse adaptée. 762 renseignements opérationnels sur des filières d'immigration ont été transmis par la DCIS. Nous avons aussi des officiers de liaison implantés stratégiquement dans des aéroports utilisés pour entrer clandestinement en France et en Europe. Ce dispositif bloque les candidats à l'immigration clandestine avant leur embarquement. Un grand nombre de documents falsifiés, contrefaits ou usurpés sont récupérés, afin qu'ils ne puissent pas, à nouveau, alimenter l'économie souterraine des faux papiers d'identité. En 2020, 7031 oppositions à l'embarquement ont été formulées et 1871 faux documents détectés. Cette thématique fait l'objet d'échanges particulièrement intenses avec la direction centrale de la police aux frontières (DCPAF) et la direction générale des étrangers en France (DGEF).

Localement, le travail de nos SSI ne s'arrête pas aux relations institutionnelles. En matière de lutte contre la pédocriminalité, notre poste en Inde est en relation avec des associations dont la vocation est de lutter contre ce fléau au niveau régional. Nos informations sont destinées à l'OCRVP (office central de répression contre les violences aux personnes) qui procédera aux enquêtes.

La lutte contre la délinquance itinérante est également un axe de travail important. Exemple, à partir de ces délits courants que sont les vols sur les chantiers

ou les cambriolages, la coordination entre notre SSI en Roumanie, la DCIS et l'OCLDI (office central de lutte contre la délinquance itinérante) est très efficace.

La DCIS participe également activement à développer une coopération opérationnelle efficace avec Israël ou les Émirats arabes unis où des délinquants de haut vol trouvent refuge et d'où ils organisent leurs trafics ou leurs escroqueries.

Par ailleurs, dans le domaine de lutte contre le trafic de stupéfiants, nous menons des coopérations exemplaires, notamment avec l'Espagne, qui permettent d'organiser des investigations communes et un échange opérationnel en temps réel.

L'identification des acteurs principaux au sein des forces de sécurité intérieure des pays partenaires grâce à la coopération technique est essentielle pour établir des échanges opérationnels de qualité, basés sur une confiance mutuelle. Les actions de coopération bilatérales sont le fruit d'échanges soutenus entre les services étrangers bénéficiaires, nos ASI, notre service central et les services de police et de gendarmerie qui réaliseront les missions. C'est un travail permanent et méthodique qui s'inscrit dans une programmation annuelle réalisée en lien avec la direction de la coopération de sécurité et de défense (MEAE/DCSD). Ce travail en amont permet de recueillir et d'analyser les besoins, mobiliser des financements, provenant en partie des ministères de l'Intérieur, de l'Europe et des Affaires étrangères et de fonds européens. La DCIS répond également à des demandes hors programmation. En 2019, 555 actions ont été réalisées en matière de lutte contre le terrorisme et 406 contre la criminalité organisée : parmi celles-ci, 71 contre la cybercriminalité et une vingtaine contre la délinquance économique et financière.

Comme vous avez pu le remarquer, la DCIS est présente en soutien de tous les services du ministère de l'Intérieur, en leur apportant analyses et informations, suivis des enquêtes et logistique nécessaire lorsque des magistrats et des enquêteurs se déplacent à l'étranger.

L.R.D.G. : Quel bilan faites-vous des actions de coopération au niveau européen et international ?

Une réponse qui passerait par l'évocation d'un bilan pour le bloc européen et d'un autre pour le « reste du monde » ne serait pas appropriée, tant l'expertise développée au fil des années par la DCIS débouche sur des actions de coopération ciblées, soit à l'échelon du pays, soit à l'échelon régional, et toujours en adéquation avec des besoins précis.

Je préfère souligner la mise en oeuvre de réponses à des problématiques de sécurité intérieure qui ont fait leur preuve dans des pays et régions crisogènes et des différentes approches de la coopération, qui peut être technique ou opérationnelle.

J'aimerais aussi revenir sur l'impact de la pandémie sur notre réseau et nos actions de coopération. Si avant la pandémie, la DCIS mettait en oeuvre en moyenne 2500 actions de coopération technique à l'année, le nombre de ces actions a été divisé par trois durant la crise. Paradoxalement, l'activité de la DCIS n'a pas pour autant diminué : notre réseau à l'étranger s'est adapté. Il a fait preuve de résilience en mettant en oeuvre, à partir des ressources disponibles en local, des formations répondant aux demandes de nos partenaires. Le lien entre la centrale et notre réseau a même été resserré grâce à l'utilisation fréquente des moyens de visioconférence.

Dans le domaine européen, les grandes lignes de notre bilan concernent d'abord notre investissement dans la préparation de la présidence française de l'Union européenne. La DCIS est chef de file pour la France sur un des groupes de travail spécialisés du Conseil dédié aux questions de police en général et où sont débattus les sujets en rapport avec l'application de la loi pénale dans les États membres. Elles concernent aussi notre action au sein du cycle politique de l'Union européenne, plus connu sous le nom d'EMPACT (*European multidisciplinary platform against criminal threats*), où des avancées sont recherchées dans les domaines de la lutte contre le trafic de stupéfiants, la criminalité organisée, la cybercriminalité ou encore la criminalité environnementale.

Enfin, à travers l'évocation des financements européens, qu'il s'agisse du fonds de sécurité intérieure pour la police (FSI-Police) ou des autres mécanismes de financement proposés par l'Union européenne pour les projets de coopération des États membres au profit de leurs partenaires étrangers, je souhaite souligner l'importance jouée par ces sommes dans notre mode de fonctionnement, mais aussi l'excellence des experts de la DCIS dans le montage

des dossiers de financement destinés à capter ces lignes budgétaires indispensables au fonctionnement de la plupart des États membres engagés dans des actions de coopération. Grâce à ces budgets qui s'agrègent aux budgets nationaux, nous sommes en capacité d'augmenter la mise en oeuvre de coopération de sécurité.

La DCIS est donc capable de développer une coopération dynamique et innovante dans le monde et de mettre en place des dispositifs performants de lutte contre la criminalité à l'échelon local ou régional et avec un fort retour en sécurité intérieure pour la France. Je termine avec l'exemple du dispositif des partenariats opérationnels conjoints (POC), formule de travail à forte valeur ajoutée sur le plan des résultats opérationnels, il a fait ses preuves, à l'image de celui du Sénégal mis en place dans le domaine de la lutte contre le trafic de migrants. C'est sur la base de cette agilité que la DCIS construit son action de coopération, qui sous-entend la création d'outils sur mesure que les partenaires vont s'approprier et faire fonctionner dans la durée.

OUVRAGES RÉCENTS

L'UNION EUROPÉENNE ET L'IMMIGRATION IRRÉGULIÈRE

AUTEUR : MARC AMSTRONG NOËL

ÉDITEUR : L'HARMATTAN

Résumé

Des noyades en cascade aux refoulements des migrants et réfugiés tentant d'atteindre les rivages de l'Europe, en passant par le développement des formes d'asile au rabais, cet ouvrage - qui conjugue la théorie et l'empirie - expose de manière circonstanciée les drames humanitaires symptomatiques de la politique migratoire de l'Union européenne en mer Méditerranée.

En vue de combler le vide de mémoire relatif à la question migratoire en Europe, il rappelle que la migration n'est pas une exceptionnalité africaine, du Proche et Moyen-Orient. Le processus de construction de la politique migratoire de l'Union européenne est retracé afin de montrer comment celle-ci, caractérisée par une philosophie à tonalité défensive, a contribué à l'instauration et à l'accélération du phénomène de l'immigration irrégulière en mer Méditerranée.

Cet ouvrage analyse également les préjugés et les discours stéréotypés qui participent de la fabrique de la peur, en Europe, de l'immigration en provenance des régions susmentionnées.

La politique migratoire de l'Union européenne n'a pas réussi le test de l'universalité des droits de l'homme.

LA LUTTE CONTRE LE TERRORISME ET LA CRIMINALITÉ ORGANISÉE EN MATIÈRE DE RENSEIGNEMENT

PAULINE BONNECARRÈRE

MAGISTRATE, CHARGÉE DE MISSION À LA COMMISSION NATIONALE DU CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT (CNCTR)

Des vagues d'attentats depuis 2015 au suivi des subversions violentes en passant par la lutte contre la cybercriminalité, l'activité des services de renseignement français n'a eu de cesse de croître, de se diversifier et d'impliquer la mise en oeuvre de moyens technologiquement innovants et humainement intrusifs.

L'année 2021 a été particulièrement riche en apports s'agissant de l'encadrement des techniques de renseignement. Si le cadre juridique avait été bien établi par la loi du 24 juillet 2015 relative aux renseignement[1], la réforme législative du mois de juillet de cette année s'est doublée d'importantes évolutions portées par les juridictions européennes. L'ensemble de ces apports a vocation à consolider le cadre légal du renseignement, notamment en renforçant les prérogatives de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

La CNCTR contrôle le respect de ce cadre légal lors de la mise en oeuvre des techniques de renseignement. Si la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques[2] prévoyait seulement l'exercice d'un contrôle restreint par la Commission nationale de contrôle des interceptions de sécurité, première autorité administrative indépendante, la CNCTR s'est vue doter de prérogatives très élargies.

Ce positionnement fait désormais de celle-ci un acteur incontournable venu sécuriser le système français aujourd'hui mis à l'épreuve par la Cour de justice de l'Union européenne et la Cour européenne des droits de l'Homme.

L'article L801-1 du Code de la sécurité intérieure prévoit que « le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité ». Ainsi, le cadre légal du renseignement est le fruit d'un équilibre subtil entre les nécessités liées à la sécurité nationale et la préservation des libertés individuelles.

Du fait même de l'exercice de leurs missions, les services de renseignement mettent en oeuvre des techniques portant atteinte à la vie privée qui nécessitent d'être encadrées. Cette mise en oeuvre doit avant tout être motivée par la défense et la promotion d'intérêts fondamentaux de la Nation limitativement énumérés à l'article L811-3 du Code de la sécurité intérieure : l'indépendance nationale, l'intégrité du territoire et la défense nationale ; les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; les intérêts économiques, industriels et scientifiques majeurs de la France ; la prévention du terrorisme ; la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à

la reconstitution de groupements dissous, des violences collectives de nature à porter gravement atteinte à la paix publique ; la prévention de la criminalité et de la délinquance organisées ; la prévention de la prolifération des armes de destruction massive. La loi du 28 février 2017 relative à la sécurité publique, en créant l'article L855-1 du Code de la sécurité intérieure, a par ailleurs prévu que les services de l'administration pénitentiaire puissent être autorisés à mettre en oeuvre certaines techniques de renseignement à l'encontre des seules personnes détenues, aux fins de prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires.

Les techniques de renseignement sont également encadrées par de grands principes qu'édicte la loi mais également par une procédure de contrôle qui tend à se développer et à s'universaliser. La multiplication des sources énonçant les éléments de cet encadrement et leur actualité nécessitent une revue permettant de clarifier leur articulation.

Il conviendra également de s'intéresser au cas spécifique de la recherche de renseignement en matière de lutte contre le terrorisme et la criminalité organisée. Connaître les compétences des services de renseignement dans une phase ayant vocation à précéder et à construire le dossier judiciaire est essentielle pour l'autorité judiciaire, à défaut de toujours pouvoir accéder au contenu des investigations réalisées en matière administrative.

La nécessité pour les services de renseignement de demeurer en pointe des différentes luttes de défense de la sécurité nationale doit être maitrisée eu égard aux enjeux majeurs en termes de libertés individuelles mais également de préservation de la prévalence du judiciaire.

Le présent s'attache ainsi à exposer le cadre légal (I), les récents apports jurisprudentiels (II) et la mise en oeuvre de passerelles entre renseignement et procédure judicaire (III).

I. L'état du droit en matière de renseignement

La loi du 24 juillet 2015 relative au renseignement[3] prévoit les conditions d'accès des services de renseignement aux techniques et le rôle de la CNCTR qui veille au respect de ces modalités. À travers différents critères légaux limitativement énoncés (A), se dessine le rôle central de la CNCTR (B).

A. Des principes directeurs affirmés et des critères légaux renforcés

Les services de renseignement sont divisés en deux catégories. D'une part, les services spécialisés de renseignement, dits du « premier cercle » que sont la direction générale de la sécurité extérieure (DGSE), la direction du renseignement et de la sécurité de la défense (DRSD), la direction du renseignement militaire (DRM), la direction générale de la sécurité intérieure (DGSI), le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) et le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin). À l'exception de la DRM et de Tracfin, les services du premier cercle ont la faculté de recourir à l'ensemble des techniques de renseignement. D'autre part, le « second cercle » regroupe les services qui peuvent se voir confier des missions de renseignement, et que sont la direction centrale de la police judiciaire, la direction centrale de la police aux frontières, la direction centrale de la sécurité publique, la direction générale de la gendarmerie nationale, la préfecture de police de Paris, la direction régionale de la police judiciaire, la direction de la sécurité de proximité de l'agglomération de Paris et la direction de l'administration pénitentiaire. Ceux-ci n'ont accès qu'à des techniques de renseignement limitativement énoncées.

Le Code de la sécurité intérieure reprend dans son livre VIII l'ensemble des textes issus de la loi renseignement du 24 juillet 2015, complétée par une loi relative à la surveillance électronique des communications internationales du 30 novembre 2015[4].

Ce livre se divise en 9 titres dédiés aux techniques et aux renseignements qu'elles permettent de recueillir, aux missions et au fonctionnement de la CNCTR, aux recours juridictionnels, à la protection des agents des services de renseignement et aux obligations des opérateurs.

Le livre VII du Code de la sécurité intérieure est introduit par l'article L801-1 précité qui innerve l'ensemble des textes et édicte le principe de proportionnalité applicable à toutes les mesures de surveillance.

Ce principe découle de l'adaptation en droit interne d'un principe énoncé et développé dans la jurisprudence européenne et ainsi résumé : *« la police ne doit pas tirer sur les moineaux à coups de canon »*[5]. Ce principe est devenu

aujourd'hui le marqueur de l'action administrative. Dans le domaine du renseignement, la CNCTR vérifie non seulement s'il existe dans les circonstances de l'espèce une menace susceptible de justifier une mesure de renseignement, mais encore si cette mesure est appropriée par sa nature et sa gravité à l'importance de la menace.

Le respect du principe de proportionnalité est doublé, pour les techniques les plus intrusives, de l'exigence de satisfaire au principe de subsidiarité, qui contraint les services à motiver leurs demandes, non seulement quant au bien-fondé de la surveillance mais également sur le choix spécifique de la technique de renseignement envisagée.

Les techniques de renseignement dont la mise en oeuvre peut être autorisée sont les accès administratifs aux données de connexion, les interceptions de sécurité, la captation de paroles prononcées à titre privé, la captation d'images dans un lieu privé, le recueil ou la captation de données informatiques, la géolocalisation d'un véhicule ou d'un objet, l'introduction dans un lieu privé. La surveillance des communications émises ou reçues à l'étranger fait l'objet de dispositions particulières[6]. Enfin, l'interception des communications échangées au sein d'un réseau ouvert empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques est autorisée[7].

La loi de 2015 a fait l'objet d'une réforme par la loi relative à la prévention d'actes de terrorisme et au renseignement du 30 juillet 2021[8] afin de tenir compte de l'évolution des technologies et des modes de communication utilisés par les terroristes.

Les services de renseignement disposent désormais de la possibilité d'intercepter des communications satellitaires grâce à un dispositif de captation de proximité.

La technique dite de l'algorithme, expérimentée depuis 2015 et autorisée jusqu'au 31 décembre 2021, est pérennisée. Cette technique permet un traitement automatisé des données de connexion et de navigation sur internet, grâce à la coopération des fournisseurs d'accès. Cette surveillance algorithmique est étendue aux adresses (URL) de connexion afin de détecter des profils à risque.

Cette réforme tire également les enseignements de plusieurs jurisprudences européennes.

La conservation des données de connexion est réformée afin de tirer les conséquences de la décision "*French Data Network*" du Conseil d'État du 21 avril 2021[9].

L'article 11 de la loi prévoit, à l'article L821-1 du Code de la sécurité intérieure, que lorsque le Premier ministre délivre une autorisation de mise en oeuvre d'une technique de renseignement après avis défavorable de la CNCTR, le Conseil d'État est immédiatement saisi et doit statuer sur la légalité de la décision du Premier ministre dans un délai de vingt-quatre heures. La décision du Premier ministre ne peut être exécutée avant que le Conseil d'État ait statué sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné sa mise en oeuvre immédiate.

Le texte prévoit enfin l'encadrement des échanges entre services de renseignements français. Si ces échanges concernent des informations poursuivant une finalité au titre de laquelle la technique de renseignement ayant permis leur recueil n'avait pas été autorisée ou si le service destinataire n'avait pas légalement accès à la technique mise en oeuvre, ces échanges font désormais l'objet d'un régime d'autorisation nécessitant un avis de la CNCTR et feront l'objet d'un contrôle de sa part. L'existence et le rôle de l'autorité administrative indépendante de contrôle sont ainsi devenus la garantie de la conformité du cadre légal français aux exigences européennes.

B. Le rôle central de la CNCTR dans le développement de l'encadrement des techniques de renseignement

L'élaboration d'un cadre juridique renforçant la protection de la vie privée et fixant les conditions dans lesquelles il peut être porté atteinte au secret des correspondances pour des motifs de police administrative trouve son origine dans une décision du Premier ministre du 28 mars 1960 créant le groupement interministériel de contrôle (GIC), service placé sous son autorité et chargé d'exécuter, pour le compte des services de renseignement, les interceptions téléphoniques administratives.

Cette création devait apporter des garanties à l'exécutif quant à la bonne utilisation des moyens d'interception par les services de renseignement, afin d'éviter des opérations de surveillance contraires aux intérêts de la France ou des autorités politiques.

La première autorité administrative

indépendante chargée de contrôler la mise en oeuvre d'une technique de renseignement a été créée par la loi du 10 juillet 1991[10] relative au secret des correspondances émises par la voie des télécommunications. Il s'agit de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), compétente à l'origine uniquement en matière d'interceptions administratives de correspondances, dites « interceptions de sécurité ». La loi du 10 juillet 1991 a été adoptée peu après que la Cour européenne des droits de l'Homme a jugé, par deux arrêts du 24 avril 1990 (affaires Huvig[11] et Kruslin[12] contre France), que le régime juridique français relatif aux écoutes judiciaires méconnaissait l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui protège le droit de toute personne au respect de sa vie privée et familiale. Outre cette condamnation, les révélations concernant « l'affaire des écoutes » exécutées par des membres de la cellule antiterroriste de l'Élysée et mises en oeuvre par le GIC ont démontré la nécessité de mettre en place un cadre légal précis et un organe de contrôle externe et indépendant.

Créée par la loi du 24 juillet 2015, la Commission nationale de contrôle des techniques de renseignement (CNCTR) est chargée du contrôle externe de la légalité de l'activité des services de renseignement. Autorité administrative indépendante, elle s'est substituée à la CNCIS et bénéficie de compétences et de prérogatives élargies par rapport à celle-ci.

La CNCTR procède à un contrôle *a priori* des demandes d'autorisation de mise en oeuvre des techniques de renseignement. Elle émet ainsi un avis à destination du Premier ministre lequel prend la décision d'autorisation de la technique. La CNCTR apprécie la compétence du service, la régularité de la procédure mais également la motivation qui doit rendre plausible le lien entre la cible et la finalité invoquée. Elle s'assure que le suivi d'un objectif respecte le principe de proportionnalité, tant dans l'emploi de la technique choisie que dans la durée de la surveillance, et donc que l'atteinte à la vie privée sollicitée est proportionnée à la gravité de la menace. Pour les techniques les plus intrusives, la CNCTR s'assure également que le renseignement recherché ne puisse être recueilli que par la mise en oeuvre de la technique demandée. La procédure encadrant les autorisations de mise en oeuvre des techniques de renseignement a été conçue pour que les demandes soient traitées dans des délais garantissant la réactivité opérationnelle des services et le plein exercice du contrôle.

La CNCTR exerce également un contrôle *a posteriori* consistant à vérifier les conditions de réalisation des techniques et contrôler les données recueillies. Ce contrôle *a posteriori* s'exerce à distance mais également sur pièces et dans les services. La CNCTR a accès à l'intégralité des données recueillies, transcrites et conservées par les services.

L'élargissement du périmètre du contrôle de la CNCTR a fait d'elle un acteur incontournable de la mise en oeuvre des techniques de renseignement. Elle rend également des délibérations sur l'ensemble des textes régissant son domaine d'exercice. La plénitude de son exercice s'avère être une sécurité pour l'ensemble des citoyens mais également pour la pérennité du cadre juridique, soumis à des exigences européennes de plus en plus fortes.

II. Les exigences des apports jurisprudentiels européens

Deux décisions des juridictions européennes sont venues bousculer le cadre légal français du renseignement en exigeant des garanties particulières, tant dans le cas de la protection des données de télécommunications exploitées à l'intérieur des États (A) que sur la question des échanges de renseignement entre services ou entre pays (B).

A. La question de la protection des données au coeur de la jurisprudence de la Cour de justice de l'Union européenne et du Conseil d'État

L'arrêt rendu par le Conseil d'État statuant en assemblée le 21 avril 2021 dit *French Data Network et autres*[13] vient tracer la frontière entre la préservation des libertés et les nécessités sécuritaires à la suite à l'arrêt *Tele2 Sverige et Watson e.a*[14] du 21 décembre 2016 rendu par la CJUE qui censurait les législations imposant aux opérateurs de télécommunication et aux fournisseurs de service en ligne de conserver l'ensemble des données de connexion des usagers.

La Cour s'était alors prononcée à l'encontre des arguments de quinze États membres parties à la procédure, de ceux de la Commission elle-même, et des conclusions de son avocat général.

Cet arrêt condamnait la législation suédoise et, par extension, celle de tous les États membres faisant l'obligation aux opérateurs de communication électronique et

aux fournisseurs de services en ligne de conserver, même pour une durée limitée, les données de connexion de leurs abonnés de manière indifférenciée, en vue de leur éventuelle réquisition par l'autorité judiciaire ou par les services de renseignement dans le but de lutter contre la criminalité. Plusieurs arrêts de la Cour ont fait suite à l'affaire « *Tele2* » dont *La Quadrature du Net e.a*[15] rendu en octobre 2020 et concernant les questions préjudicielles françaises.

Toutes les techniques de renseignement n'étaient pas concernées par l'application du droit de l'Union européenne, les interceptions de sécurité, et les autres techniques ne nécessitant pas la collaboration des opérateurs, ayant été écartées par le Conseil d'État dans ses questions préjudicielles.

S'agissait-il alors de ne remettre en cause que des techniques de renseignement secondaires ? Loin s'en faut.

Les traitements automatisés, qui s'appliquent de manière globale à l'ensemble des personnes faisant usage des moyens de communications électroniques, ont, d'une part, retenu l'attention de la Cour. La CJUE a estimé qu'une telle ingérence n'était proportionnée que si un État membre se trouvait face à une menace grave pour la sécurité nationale, réelle, actuelle ou prévisible, et si la durée de la conservation était limitée au strict nécessaire. Cette position a conduit la CJUE à considérer que l'utilisation faite des traitements automatisés de données pour la sauvegarde de la sécurité nationale méconnaissait le droit de l'Union.

De même, elle a considéré que le recueil en temps réel des données relatives au trafic ou à la localisation n'était conforme au droit de l'Union que s'il était mis en oeuvre en raison d'une menace grave pesant sur la sécurité nationale, c'est-à-dire à l'égard des personnes pour lesquelles il existait une raison valable de soupçonner qu'elles étaient impliquées d'une manière ou d'une autre dans des activités terroristes.

Pour la mise en oeuvre de l'ensemble des techniques de renseignement impliquant l'accès aux données de connexion évoquées ci-dessus, la Cour a exigé que celles-ci soient soumises à un contrôle préalable effectué par une juridiction ou par une entité administrative indépendante rendant une décision dotée d'un effet contraignant. Cette position de la Cour l'a amenée à constater une violation du droit de l'Union tant dans le cas français, la CNCTR rendant des avis simples sur la mise en oeuvre des techniques de renseignement, que dans le cas estonien, le Ministère public autorisant les services judiciaires à accéder aux données de connexion pour les besoins des enquêtes pénales.

Alors que les personnalités auditionnées par le Conseil d'État avaient largement fait part de leur inquiétude quant aux conséquences de la transposition de la jurisprudence de la CJUE sur le déroulement des enquêtes, celui-ci est venu valider l'équilibre français en jugeant que la conservation généralisée des données était actuellement justifiée par la menace existante pour la sécurité nationale.

Le Conseil d'État a estimé que l'encadrement de la conservation des données par le droit européen ne remettait pas en cause les exigences constitutionnelles relatives à la sécurité nationale et à la lutte contre la criminalité grave. Selon lui, l'objectif de sauvegarde de la sécurité nationale recouvrait la majorité des missions des services de renseignement français. Par ailleurs, il a relevé que la menace pesant sur la sécurité nationale était effectivement réelle, actuelle et intense, comme l'exigeait la Cour, et qu'elle était protéiforme. Il a ainsi pris en compte des menaces plus variées que celle retenue par la Cour, superposant à la menace terroriste d'autres atteintes graves à prévenir, comme l'espionnage industriel et politique, ou l'émergence de groupuscules extrémistes et violents sur le territoire national.

Il a toutefois relevé que le cadre légal français, en ne prévoyant pas un réexamen périodique des risques pour la sécurité nationale de la nécessité de maintenir cette obligation de conservation au moins tous les ans, méconnaissait le droit de l'Union.

En outre, le Conseil d'État a jugé qu'une conservation ciblée des données de connexion, telle qu'exigée par la CJUE, se heurterait à des difficultés techniques qui pourraient compromettre sa mise en oeuvre et même présenter un intérêt opérationnel incertain. Le Conseil d'État a estimé que cette conservation de données, postérieure aux évènements la justifiant, ne permettait pas de garantir le respect des objectifs constitutionnels que sont, en France, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions pénales.

En outre, la juridiction française

a relevé que ces données de connexion auxquelles accèdent les autorités judiciaires ou de renseignement étaient initialement conservées au titre de la sauvegarde de la sécurité nationale. Dès lors, s'il ne peut être légalement imposé aux opérateurs de conserver l'ensemble des données de connexion au titre de la lutte contre la criminalité et de la prévention des menaces à l'ordre public, les autorités judiciaires et les services de renseignement peuvent tout de même accéder aux données retenues indistinctement par les opérateurs.

Quelles conséquences sont à tirer de cette position, bien différentes selon que l'on se trouve dans une phase judiciaire ou de renseignement ?

La France a opéré une distinction entre la conservation des données et l'accès à celles-ci : si la conservation des données de connexion ne peut être légalement ordonnée qu'en vue d'assurer la sécurité nationale, l'accès à ces données initialement conservées peut être autorisé pour des motifs distincts, comme la lutte contre la criminalité et le maintien de l'ordre public.

La principale carence du dispositif français relevée par le Conseil d'État est que la CNCTR n'émet qu'un avis simple sur la mise en oeuvre de ces techniques et que la saisine de la formation spécialisée du Conseil d'État ne lui est, le plus souvent, ouverte qu'après l'autorisation accordée par le Premier ministre. Sur ce point, le Conseil d'État a conclu à une violation du droit de l'Union.

La loi du 30 juillet 2021[16] prévoit donc une modification du contrôle préalable aux recueils de données effectués par les services de renseignement. Toute autorisation du Premier ministre donnée aux services de renseignement qui serait délivrée après un avis défavorable de la CNCTR provoquera la saisine automatique du Conseil d'État, qui statuera dans un délai de vingt-quatre heures sur la légalité de cette autorisation. L'autorisation du Premier ministre ne pourra pas être exécutée avant que le Conseil d'État ait statué, sauf en cas d'urgence dûment justifiée. Outre les effets renforcés de ses décisions, la CNCTR va voir le périmètre de son contrôle étendu.

B. *Big Brother watch*, les interceptions de masse et d'échanges de renseignements entre services étrangers saisies par la CEDH

Les arrêts de la Grande chambre de la CEDH du 25 mai 2021 Big Brother Watch et autres C/ Royaume-Uni[17] et Centrum för rättvisa C/ Suède[18] fixent la jurisprudence européenne en matière d'interceptions de masse et d'échanges de renseignements entre services étrangers.

La Cour a relevé que sept États parties à la Convention, dont la France, ont officiellement mis en place des régimes d'interception de communications en masse acheminées par câble ou voie aérienne. Il s'agit d'interceptions non ciblées. En France, deux dispositifs peuvent être regardés comme des dispositifs d'interceptions de masse : les traitements automatisés dits « algorithmes » et la surveillance des communications électroniques internationales. « L'interception en masse est d'une importance vitale pour les États » admet la CEDH.

La Cour a jugé cependant que ce régime doit faire l'objet d'un encadrement renforcé. Abandonnant son approche globale des garanties, elle exige désormais que ce régime soit encadré par des garanties « de bout en bout », c'est-à-dire appréciées à chaque étape du processus.

Ces garanties « de bout en bout » imposent aux États membres que leur cadre légal soit accessible au public, effectif et exhaustif : la loi doit prévoir l'ensemble des étapes de fonctionnement de la surveillance et les garanties de contrôle qui doivent les jalonner. En particulier, l'autorisation d'interceptions de masse et leur contrôle doivent être confiés à un juge ou à un organe indépendant.

À noter que si la Cour se prononce sur les échanges de renseignements obtenus à partir d'interceptions de masse et à la demande d'un service de renseignement, son raisonnement s'applique de la même façon à toutes les données transmises ou reçues par les États, issues d'interceptions ou non.

Quels enseignements le législateur doit-il tirer de cette position ?

À l'aune de ces nouveaux critères, la Cour a conclu que la réglementation britannique souffrait de plusieurs carences. S'agissant de la procédure d'autorisation de la surveillance de masse, les autorisations d'interception britanniques n'étaient pas délivrées par un juge ou un organe indépendant et les critères utilisés pour discriminer les communications interceptées à exploiter n'étaient pas suffisamment précisés et contrôlés. Elle en a conclu que les stipulations de l'article 8 de la Convention avaient été méconnues.

Quant au régime d'interceptions de masse suédois, la Cour n'a

relevé aucune violation de la Convention par les règles de contrôle et de mise en oeuvre des interceptions de masse mais a estimé, en application de sa nouvelle approche exigeant des garanties « de bout en bout », que le contrôle *a posteriori* présentait une insuffisance structurelle et que l'existence de plusieurs contrôles alternatifs n'était pas suffisante pour considérer que les justiciables disposaient d'un recours effectif.

La Cour exige que les demandes de transmission d'informations adressées aux pays étrangers aient un fondement en droit interne, accessible et prévisible quant à ses effets. Cette base légale doit, en outre, indiquer dans quelles circonstances et sous quelles conditions les autorités sont habilitées à formuler de telles demandes et prévoir des garanties effectives.

Elle précise que, dès la réception des éléments interceptés, l'État destinataire doit mettre en oeuvre des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction. Le recours à un tel dispositif doit également être soumis à une supervision indépendante et à un contrôle *a posteriori* indépendant.

La Cour pose plusieurs autres conditions. Le droit interne doit prévoir clairement les circonstances dans lesquelles le transfert peut être réalisé et l'État émetteur doit s'assurer de la mise en place, par l'État destinataire, de garanties suffisantes pour prévenir les abus et les ingérences disproportionnées, notamment en restreignant la divulgation des informations à d'autres parties et en accordant une protection particulière aux renseignements sensibles (comme les éléments journalistiques confidentiels). Enfin, la Cour exige que le transfert d'informations à des partenaires de renseignement étrangers soit soumis à un contrôle indépendant.

La Cour a indiqué qu'elle appréciera « globalement » le caractère suffisant de chaque cadre juridique. Le jugement des requêtes concernant le cadre juridique français ayant été suspendu dans l'attente des arrêts de la Grande chambre, l'appréciation du cadre juridique français devrait intervenir dans les prochains mois.

L'encadrement des échanges avec les services étrangers est un rendez-vous législatif à venir en matière de renseignement.

III. La mise en oeuvre des passerelles entre renseignement et procédure judicaire

Il convient de distinguer deux situations distinctes : la judiciarisation d'un renseignement que la mise en oeuvre de techniques avait pour objectif d'étayer (A) et le traitement d'une information découverte incidemment dans le cadre d'investigations portant sur d'autres faits (B).

A. Le traitement de l'information spécifiquement recherchée

Les renseignements exploités sous l'égide du Code de la sécurité intérieure en matière de contre-terrorisme et de lutte contre la criminalité organisée ne peuvent l'être que dans un cadre préventif, comme l'énonce l'article L811-3 du Code de la sécurité intérieure, le judiciaire conservant sa prévalence sur l'administratif. Ainsi la question de la judiciarisation du renseignement est un enjeu majeur tant pour les services de renseignement que pour les parquets.

Le fait de débuter une enquête par la mise en oeuvre de techniques de renseignement présente des avantages notables. Elle permet notamment d'effectuer des levées de doutes ainsi que de vérifier, étayer et « blanchir » le renseignement initial. Elle va également permettre de mettre en oeuvre des techniques qui ne sont pas prévues par le Code de procédure pénale.

La frontière entre prévention et caractérisation de l'infraction est cependant parfois difficile à fixer, notamment pour les services ne disposant pas de la « casquette » judiciaire.

La CNCTR, dans le cadre de l'exercice de son contrôle de légalité *a priori* et *a posteriori*, est garante du respect de la prévalence du judicaire et veille à recommander aux services de judiciariser les dossiers lorsque les éléments constitutifs semblent réunis. Elle peut même aller jusqu'à émettre un avis défavorable à la mise en oeuvre ou au renouvellement d'une technique de renseignement si elle estime que les faits sont suffisamment caractérisés et doivent être appréhendés dans un cadre judiciaire.

La judiciarisation d'une affaire, initiée en matière administrative et ayant entraîné la mise en oeuvre de techniques de renseignement, doit être soumise au parquet compétent.

Une différence majeure réside dans le fait que les magistrats du parquet national anti-terroriste dirigeant les enquêtes de contre-terrorisme bénéficient d'une habilitation au secret de la défense nationale, ce qui n'est pas le cas

des magistrats de la juridiction nationale chargée de la lutte contre la criminalité organisée ou des juridictions interrégionales spécialisées. Les premiers sont donc en mesure d'être bien plus largement informés que les seconds. Ce point ne peut qu'interroger quant à la prise en compte des besoins de l'institution judiciaire et est à mettre en perspective avec les difficultés d'intégration du renseignement inopinément découvert dans la procédure judiciaire.

B. Le traitement de l'information inopinément découverte

L'exploitation de techniques de renseignement peut amener les services à découvrir des éléments concernant des faits délictuels ou criminels commis et qui relèvent donc de la compétence exclusive de l'autorité judiciaire. Cette situation n'est explicitement prévue par aucun texte, les énonciations de l'article 40 du Code de la procédure pénale venant se heurter à la problématique de la préservation du secret de la défense nationale.

La protection du secret de la défense nationale repose sur un corpus juridique qui a récemment fait l'objet d'une importante révision avec une modification des articles R2311-2 et suivants du Code de la défense et une nouvelle instruction générale interministérielle n°1300 applicables depuis le 1er juillet 2021. La réforme adopte un nouveau système de classification à deux niveaux, Secret et Très secret et supprime le niveau Confidentiel défense. Le niveau Secret s'applique aux informations et supports dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale. Le niveau Très Secret s'applique aux informations et supports dont la divulgation ou auxquels l'accès auraient des conséquences exceptionnellement graves pour la défense et à la sécurité nationale.

L'accès à des informations classifiées est limité aux personnes bénéficiant d'une habilitation d'un niveau suffisant et ayant besoin d'en connaître dans le cadre de leurs fonctions. Le fait de rendre public un secret protégé ou d'en prendre connaissance constitue le délit de compromission.

Il est légitime de s'interroger sur le fait de savoir comment les acteurs de la justice, qui ne sont pas habilités, peuvent concourir avec efficacité à sa mission de manifestation de la vérité sans avoir accès à certains éléments issus de la mise en oeuvre de techniques de renseignement.

Si l'article L2312-4 du Code de la défense organise une procédure spécifique de déclassification soumise à la Commission du secret de la défense nationale, autorité administrative indépendante qui peut être saisie par une juridiction, cette procédure implique que l'autorité judiciaire ait eu connaissance de l'information et de sa présence dans des documents classifiés.

Il convient cependant de rappeler que la décision de classification d'une information et le niveau de cette classification relèvent des services de renseignement eux-mêmes. Un service de renseignement peut ainsi décider de communiquer l'information dont il a eu connaissance par la mise en oeuvre d'une technique de renseignement à un service de police judiciaire ou au magistrat en charge de l'enquête, sans se soumettre à cette lourde procédure. C'est donc à tort que certains services se censurent parfois, pensant qu'il ne leur est pas loisible de communiquer à un acteur judiciaire une information spécifique tirée de la mise en oeuvre de techniques de renseignement.

L'article 706-25-2 du Code de procédure pénale prévoit une dérogation à l'article 11 du même code et permet aux procureurs ayant connaissance, dans le cadre d'une procédure judicaire, d'éléments qui intéressent la prévention du terrorisme de les communiquer aux services de renseignement. Cette exception permettant d'opérer une bascule du judiciaire vers l'administratif a été étendue par la loi du 30 juillet 2021[19] à la Juridiction nationale chargée de la lutte contre la criminalité organisée. L'article 706-105-1 du Code de procédure pénale lui permet désormais, dans le cadre d'enquête visant des faits de trafic de stupéfiants, de traite des êtres humains, de trafics d'armes et explosifs ainsi que d'aide au séjour en bande organisée, de communiquer aux services de renseignement des éléments découverts et entrant dans le champ de la prévention de la criminalité et de la délinquance organisée. Cette possibilité de transférer des éléments judiciaires aux services spécialisés a également été prévue en matière de cyberattaques.

L'existence de ces textes répond à un vide juridique apparu dans la pratique des parquets concernant le traitement d'informations dont le contenu ne permettait pas l'ouverture d'une enquête judicaire mais qui s'inscrivaient précisément dans le cadre de la prévention du terrorisme et de la criminalité organisée. Il est cependant notable de

relever que la loi sécurise désormais la transmission du judiciaire vers l'administratif mais demeure trop taiseuse sur le mouvement inverse.

Une réflexion générale quant à l'habilitation des magistrats mériterait d'être engagée. En effet, il peut paraître étonnant que les magistrats, directeurs d'enquête, soient moins informés que les services enquêteurs et qu'il existe un décalage selon les contentieux traités. La question même d'une habilitation statutaire pourrait être posée. En effet, il peut apparaître contraire à la séparation des pouvoirs qu'un magistrat se voit éventuellement privé de compétences par l'effet d'un refus d'habilitation alors même qu'il a été nommé par décret afin d'occuper des fonctions définies.

De la même manière, les magistrats administratifs, qui doivent juger de la légalité d'actes fondés sur des éléments recueillis grâce à des techniques de renseignement (contentieux des MICAS (mesures individuelles de contrôle administratif de surveillance) par exemple se trouvent régulièrement placés dans la situation de devoir se prononcer à partir de notes blanches dont ils ne peuvent apprécier la réalité matérielle du contenu.

Cette situation n'est pas sans rappeler la période où les juges correctionnels étaient amenés à exercer un contrôle de légalité des arrêtés préfectoraux ordonnant les perquisitions administratives… Sans pouvoir accéder à aucun élément ayant motivé ces arrêtés. Cette situation avait conduit à l'annulation de nombre de ces perquisitions administratives et insécurisé considérablement le travail réalisé dans le cadre de l'état d'urgence.

De la même manière que certaines personnalités (ministres, hauts fonctionnaires) sont habilitées du simple fait de leur nomination, l'habilitation des magistrats ayant besoin de connaître d'informations classifiées dans le cadre de l'exercice de leur mission constituerait une avancée majeure dans l'affirmation nécessaire de la prévalence du judiciaire sur l'administratif.

Notes :

1. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.
2. Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.
3. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.
4. Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.
5. Cette expression datant de 1912, émane du commentaire du juriste allemand Fleiner de la décision Kreuzberg du 14 juin 1882 de la Cour administrative suprême de Prusse.
6. articles L. 854-1 à L. 854-9 du Code de la sécurité intérieure.
7. articles L. 855-1 A à L. 855-1 C du Code de la sécurité intérieure.
8. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.
9. Conseil d'État, Ass., 21 avril 2021, n° 393099.
10. Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances.
11. CEDH, 24 avril 1990, 11105/84.
12. CEDH, 24 avril 1990, 11801/85.
13. Conseil d'État, Ass., 21 avril 2021, n° 393099.
14. CJUE, 21 décembre 2016, aff C-203/15.
15. CJUE, 6 octobre 2020, aff C-511/18.
16. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.
17. CEDH, gr. ch., 25 mai 2021, n°s 58170/13, 62322/14 et 24960/15.
18. CEDH, gr. ch., 25 mai 2021, n°35252/08.
19. Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

LA REVUE DU GRASCO

Numéro ISSN : 2272-981X

Université de Strasbourg, UMR-DRES 7354

11, rue du Maréchal Juin - BP 68 - 67046 STRASBOURG CEDEX

Site internet : http://www.GRASCO.eu— http://www.larevuedugrasco.eu

Adresse mail : information@grasco.eu

Directrice de la revue du GRASCO : Chantal CUTAJAR

Rédactrice en chef : Jocelyne KAN

Rédacteur adjoint—Conception : Sébastien DUPENT

COURTIERS DU CRIME

QUENTIN MUGG[1]

SENIOR SPECIALIST, EU DRUGS UNIT – EUROPOL

Depuis 2020, une succession d'enquêtes d'ampleur mondiale sont venues confirmer de façon irréfutable le quasi-monopole que des opérateurs occultes détiennent dans le rapatriement et la dissimulation des profits du trafic international de stupéfiant. Leurs activités dépassent de loin le blanchiment stricto sensu et s'étendent aux aspects logistiques du trafic tout en offrant des débouchées pour les profits générés par d'autres infractions, sans lien apparent avec la drogue.

Ils sont les courtiers du crime organisé, rouages essentiels du trafic.

Personnages clé du blanchiment de l'argent de la drogue, les courtiers tiennent leur réputation et leur fortune de leur capacité à entremettre. Ils savent où trouver du cash, qui veut s'en défaire, qui en a besoin, comment le transférer d'un pays à un autre, comment le transformer et le vendre. Ils connaissent la provenance et la destination de l'argent. L'origine criminelle des fonds leur importe peu et s'ils se spécialisent sur une activité criminelle en particulier, ils le font davantage par manque d'opportunité que par choix.

Ces courtiers sont principalement des opérateurs de compensation informelle dont les mécanismes n'ont plus besoin d'être expliqués. Qu'ils s'appellent *hawaladar* au Moyen-Orient, *sarafs* au Maghreb, *brokers* en Colombie et aux États-Unis, ou *doleiros* au Brésil, tous opèrent de la même manière et transfèrent des fonds, souvent sans avoir à les transporter physiquement, grâce à des relais aux quatre coins du monde. Ce système simple à comprendre a été décrit mille fois : le courtier collecte de l'argent d'une source en un point, remet une somme équivalente d'une autre source ailleurs et prélève une commission au passage pour se dégager une marge. Simple et efficace… en théorie.

La plupart des courtiers, qu'ils soient établis en Europe, au Moyen-Orient, au Maghreb, en Amérique du Sud ou ailleurs, utilisent des méthodes similaires. Ils collectent des fonds, les assurent et les rendent disponibles au moyen d'opérations *cash to cash* ou *cash to bank* qui paraissent extrêmement simples et pour tout dire archaïques au premier abord. À première vue, le principal élément de complexité des transactions semble tenir à leur caractère international et à leur réalisation dans des lieux difficiles en termes de coopération judiciaire.

La pratique est bien différente et certains points méritent qu'on s'y attarde.

Nous aborderons donc spécialement les questions des commissions variables, du taux de change et de l'assurance. Ces points doivent être mis en perspective avec d'autres réalités que sont les consortiums de courtiers, les prêts entre opérateurs et les *cash pools.* Ces dernières sont une nécessité dans le rééquilibrage périodique des comptes de courtiers opérant des transactions collaboratives qui ne sont ni linéaires ni corrélées. Ceci nous permettra de définir plus précisément le rôle de certains courtiers dans la réalisation même des infractions. Sans verser dans la psychologie criminelle, il ne sera pas inintéressant de tenter

d'explorer, même en surface, la manière dont ces courtiers se perçoivent eux-mêmes et le contexte humain dans lequel toutes ces transactions s'opèrent.

Enfin, face à l'ampleur du phénomène, nous évoquerons des moyens mis en oeuvre pour lutter efficacement contre ces réseaux structurés.

Un maillage mondial et collaboratif

Pour le dire simplement, il est rare que les fonds collectés soient ceux remis.

À l'image des clients honnêtes d'une banque légitime, les criminels sont généralement ignorants des mécanismes à l'oeuvre dans le déplacement de leur argent. Leurs exigences de rapidité imposent aux courtiers de puiser dans des réserves immédiatement disponibles. Ce sont les *cash pools.* Il s'agit de stocks d'argent liquide que les courtiers alimentent dans les pays où ils opèrent et qu'ils utilisent en fonction des besoins.

Dans les faits, de nombreux courtiers s'associent ponctuellement pour satisfaire des demandes inverses permettant d'évacuer les fonds d'un client en les remettant à un second qui souhaite en rapatrier.

Il faut donc constamment équilibrer les comptes entre courtiers. Cet équilibrage n'intervient pas au coup par coup mais généralement sur une période fixe variant de 10 jours à un mois selon l'intensité des échanges. L'opération consiste simplement, pour chaque courtier, à regrouper les opérations de la période et déterminer le delta entre les fonds reçus et remis pour le compte de tel ou tel associé. Seule la différence est transférée au moyen d'un règlement bilatéral entre deux courtiers ou multilatéral entre plusieurs d'entre eux. Ces paiements peuvent être réalisés en valeur par le biais de transactions commerciales, opérés via le système bancaire, ou réglés en espèces par l'intermédiaire de transporteurs de fonds transfrontaliers.

Les réserves des *cash pools* peuvent être importantes car, selon une évaluation tirée de dossiers récents, la transaction moyenne représente environ 150.000 euros. Certains opérateurs déplacent plusieurs millions par semaine et le record actuel dépasse les 50 millions par mois pour un unique courtier.

Une symbiose criminelle

De telles sommes, à répartir dans de nombreux pays, nécessitent donc souvent l'intervention de plusieurs courtiers, des prêts entre opérateurs, voire la mutualisation de fonds. Fréquemment les transferts de fonds s'appuient sur des transactions en cascade, de l'import-export de marchandises, du transport physique de fonds, de la vente à la découpe de contrats de change, de l'affacturage ou encore des investissements sans qu'aucune de ces méthodes n'aient nécessairement abouties au moment de la compensation des sommes reçues, ni que le client en soit conscient ni avisé. On comprend donc qu'à défaut d'informations précises acquises au coeur même de ces réseaux, retracer le flux financier devient très complexe.

Pour le client, en revanche, les choses sont simples. Il bénéficie d'une transaction en miroir, quasiment instantanée qui ne laissera aucune trace, peu lui importe les mécanismes mis en oeuvre pour y parvenir. Il reste indifférent au fait que certains courtiers avancent de l'argent, que d'autres en investissent une partie pour augmenter leurs profits et empruntent à leurs pairs de quoi finaliser une transaction, puisqu'une nouvelle collecte vient rembourser une opération antérieure réalisée au profit d'autres clients. Qui récupèrera ces euros en Europe ? D'où proviennent les Dirhams remis à Dubaï en échange ? Cela ne le concerne pas.

Dans ces conditions, *« suivre l'argent »,* qui ne bouge pas, devient un mantra un peu simpliste difficile à mettre en oeuvre dans ce lacis de compensations et de transactions internationales et informelles. Dans la mesure où les opérations peuvent porter, comme nous l'avons découvert, sur un milliard d'euros annuel pour un unique courtier, le défi est de taille et ne peut être relevé sans une intense coopération internationale.

À ce qui précède s'ajoute le contexte historique et règlementaire des pays depuis lesquels une grande partie des transactions sont opérées. Beaucoup d'acteurs économiques ont recours aux services de courtiers pour effectuer des transferts d'argent, de façon plus souple et à des tarifs plus avantageux que dans une banque officielle.

Ainsi, les courtiers jouissent d'une réputation et d'une confiance parfois supérieure aux institutions financières régulées, ce qui leur permet de disposer, par exemple, de sommes considérables provenant de travailleurs immigrés non bancarisés, d'individus soucieux

d'éviter l'impôt et souhaitant exfiltrer des fonds pour les thésauriser ailleurs en secret. Le système se renforce aussi en s'appuyant sur le contexte local des pays dans lesquels le *courtier* opère. Certains d'entre eux pratiquent un strict contrôle des changes. La population locale et immigrée a donc de gros besoins de conversion et de transferts de fonds. Une partie de la clientèle souhaite éluder des droits d'importation fortement taxés, notamment au Maghreb. Il devient tentant pour eux d'exfiltrer leur argent à l'étranger pour y régler, souvent en espèces, des marchandises qui seront importées en sous-facturation, réduisant d'autant les droits de douane. Le courtier répond à ces besoins grâce à d'autres fonds occultes et disponibles en grande quantité, souvent ceux du trafic, et l'argent provenant des autres sources vient en compensation des sommes perçues de criminels.

La valeur et la réputation du courtier reposent donc essentiellement sur l'étendue et la fiabilité de son réseau de clients. Un double réseau. Le premier, en amont, pour collecter l'argent liquide, le second, en aval, pour lui trouver des débouchés. Ces deux réseaux sont parfois ancrés dans des univers sans rapport l'un avec l'autre. Le courtier est un entremetteur qui met en relation ces différents univers. Il est à l'aise partout, dans tous les milieux.

Les courtiers sont moins banquiers que complices

Il serait toutefois faux de supposer que les courtiers se bornent à réaliser des transferts et à organiser des « swaps ». Leur fonction dans la logistique criminelle va bien au-delà et comprend entre autres : la création ou le contrôle des sociétés utilisées dans les opérations de transports maritimes liées au trafic, le paiement des fournisseurs/producteurs de drogues au moyen du produit de trafics antérieurs, l'organisation de la logistique internationale de groupes criminels de portée mondiale. Le courtier est un rouage essentiel de la mécanique criminelle. Il n'est pas rare de le voir prendre littéralement en main des aspects logistiques cruciaux tels que la mise en place de lieux de stockage fiables ou le transport de la drogue, ce qui participe à effacer un peu plus la frontière entre le blanchiment et la complicité de trafic international de stupéfiants.

La confiance que lui accordent ses clients amène aussi le courtier à proposer des stratégies d'investissement sur le long terme permettant un blanchiment efficace au sens où on l'entend habituellement : la justification mensongère de l'origine des fonds. Ainsi, paradoxalement, mais comme souvent dans le monde criminel, l'honnêteté est une valeur cardinale du métier de courtier criminel.

Cette confiance découle aussi en partie du rôle d'assureur du courtier. S'il perd les fonds confiés, quelle qu'en soit la cause, un vol, une perte, un accident ou une saisie, il s'arrangera pour que rien ne transparaisse et remettra généralement la somme promise au client, sans dire un mot de sa mésaventure.

Tout ceci a un prix.

Les tarifs pratiqués par les courtiers intègrent donc le coût de la main d'oeuvre, des frais, de l'assurance et une part de profit. Les commissions varient de 3 à 15%, selon le service rendu et les lieux de collecte et de remise. De nombreux exemples tendent à démontrer que ces montants font l'objet d'un consensus entre opérateurs. Donner du cash contre du cash est par exemple moins coûteux que de donner du cash contre un virement bancaire sur un compte. Mais collecter des fonds aux Pays-Bas coûte bien moins cher que de le faire en France, et en remettre en Colombie est plus abordable que de le faire au Pérou. Le secteur est donc concurrentiel mais les plus gros opérateurs exercent une forme de contrôle des prix qui s'imposent aux courtiers plus modestes, lesquels dépendent souvent des premiers pour décrocher des contrats.

L'atténuation des risques - Consortium et assurances

L'industrie du blanchiment a développé une structure hiérarchique essentiellement divisée en trois niveaux. Le premier niveau correspond aux courtiers contrôlant des structures internationales et d'un réseau de correspondants mondial. Ils traitent directement avec les groupes criminels. Le deuxième niveau regroupe des individus qui ont la capacité de recevoir l'argent de la drogue à l'étranger, de le faire passer en contrebande, de l'investir (dans des biens à échanger) et/ou de le placer dans le système bancaire. Le dernier niveau comprend des individus qui fournissent des devises étrangères à leur clientèle. Ces courtiers achètent et vendent les devises aux courtiers de niveau 2.

Cette présentation est évidemment simplifiée et le système n'est pas structuré de manière très rigide. Par exemple, certains

courtiers peuvent exécuter eux-mêmes la plupart ou la totalité des fonctions ce qui présente un avantage significatif en termes de profits... mais augmente les risques.

L'acceptation d'un *contrat de blanchiment d'argent*, car c'est de cela qu'il s'agit, pour le compte de criminels comporte évidemment des risques financiers. Pour cette raison, tous les niveaux de courtiers en argent sont prêts à prendre une plus petite part des bénéfices afin de transférer le risque au courtier suivant.

Par exemple, un courtier de niveau 1 accepte un contrat pour rapatrier à Dubaï 5 millions d'euros situés en Belgique et aux Pays-Bas. Si ce courtier de niveau 1 a la capacité de traiter 5 millions d'euros, il gagnera la commission accordée par le client, mais il assumera tous les risques de perte. Il est probable qu'il vende une partie, sinon la totalité, de ces 5 millions d'euros à un ou plusieurs courtiers de niveau 2 qui contrôlent les cellules de blanchiment d'argent dans les pays concernés. Toutefois, pour les mêmes motifs d'atténuation des risques ou de manque de clientèle, ces courtiers de niveau 2 peuvent à leur tour vendre tout ou partie des euros de la drogue à des courtiers de niveau 3, qui ont des clients ayant besoin de ces euros. Comme le courtier de niveau 1, le courtier de niveau 2 vendra les devises au courtier de niveau 3 à un taux plus élevé que celui auquel il les a achetées, ce qui lui permet de réaliser un bénéfice.

L'événement clé de l'ensemble du cycle d'événements décrit ci-dessus est la réception initiale de l'argent de la drogue par le courtier. À ce stade, le trafiquant est assuré de recevoir le paiement de la valeur de ces euros, moins la commission.

Les enquêtes nationales ciblent fréquemment des opérateurs de niveau 3 qui se défendent d'être des blanchisseurs considérant qu'ils bougent juste d'un point à un autre, de manière certes informelle ou traditionnelle, de l'argent dont ils se soucient peu de l'origine et dont ils ignorent effectivement totalement la provenance exacte. Tout ceci se produit en espèces. Avec eux, pas de *« cycle du blanchiment »*. Ils reçoivent du cash et le restituent.

Quel que soit leur niveau, pour les courtiers, le risque et la responsabilité commencent au moment où ils perçoivent l'argent. Autant dire qu'une proportion importante des saisies d'argent de la drogue vient en réalité s'imputer au chiffre d'affaires du courtier et non aux trafiquants.

Le blanchiment 2.0

Et la crypto-monnaie ? Les données disponibles indiquent qu'elle est de plus en plus répandue dans les opérations de blanchiment. Les transactions sont généralement *« Peer to Peer »* auprès de revendeurs acceptant des espèces en grande quantité principalement contre du Bitcoin, des « stables coins », de l'Ethereum et du Monero, le tout pour une faible commission de l'ordre de 1%. Ces crypto-monnaies sont généralement utilisées comme moyen de transfert mais certains commencent à s'en servir comme moyen de thésaurisation et d'investissement. Cette émergence de la crypto-monnaie traduit une réalité plus vaste : l'adoption en cours de ces nouvelles valeurs et de ces moyens de paiement par la société civile en induit mécaniquement l'adoption par le monde criminel. Jusqu'à présent la même chose s'est produite avec les billets de banque sans que personne n'appelle à leur interdiction.

Bien sûr, nos enquêtes montrent que les schémas utilisés par les blanchisseurs peuvent être d'une infinie variété, combinant des comptes bancaires, des montages financiers internationaux, des sociétés écrans *offshore*s, l'utilisation de nombreux prête-noms et mille autres artifices. Néanmoins, une grande partie des transactions consistent tout simplement en de multiples collectes et remises déportées.

La lutte contre le blanchiment de l'argent de la drogue : un défi collectif et européen

Bien sûr, en bout de chaîne, le produit du crime réintègrera au moins en partie le système financier officiel. Mais l'éventuelle enquête qui découlerait d'une déclaration de soupçon, intervenue au stade lointain du réemploi de fonds, buterait inévitablement sur l'internationalisation des opérations impliquant du cash et des marchandises. Dans l'éventualité où un flux bancaire serait remonté au prix d'une longue enquête internationale, l'origine des fonds resterait à jamais un mystère, car le point d'introduction de l'argent dans le système bancaire se situe toujours à l'étranger, dans un pays très éloigné de la source d'origine et de l'infraction initiale.

L'expérience montre que pour s'attaquer efficacement aux réseaux actifs et structurés, c'est au niveau européen qu'il convient d'agir, car tous les dossiers sont

au moins à cette échelle : celle d'une criminalité organisée transnationale couplée à une chaîne logistique souvent autonome incluant le blanchiment. Par ailleurs, l'Europe est devenue le premier marché de la drogue et les profits générés sur notre continent alimentent une foule d'autres activités criminelles en rendant les fonds disponibles au moyen des mécanismes décrits plus haut.

Les moyens de la lutte

Face à l'ampleur du phénomène, le développement des enquêtes financières, en parallèle des dossiers sur les crimes générant ces profits, est maintenant devenu habituel. Pourtant ces circuits financiers frauduleux échappent fréquemment aux outils de détection, de contrôle et de surveillance dont nous disposons. Les courtiers se spécialisent volontiers sur la circulation d'espèces et évitent les circuits bancaires de nos juridictions. Ainsi, il est crucial de rechercher activement les réseaux de blanchiment et de ne pas se limiter à des investigations découlant d'une affaire portant sur l'infraction préalable au blanchiment.

Une démarche proactive prévaut de plus en plus au niveau européen. Elle repose sur le partage de l'information et la mise en oeuvre de techniques spéciales d'enquête.

Les deux principales difficultés auxquelles se heurte la lutte contre ces blanchisseurs sont donc la nature éminemment internationale des opérations et la difficulté de surveiller les nombreux moyens de communication.

Sur le plan des communications, sans entrer dans les détails, on peut souligner la nécessité, encore récemment démontrée par les phénoménaux dossiers Encrochat, Sky et Anom, de rester à niveau dans la course technologique.

Parallèlement à ces défis techniques, des méthodes d'enquêtes plus traditionnelles apportent des solutions efficaces pour la traque de l'argent sale, au premier rang desquelles se trouve l'infiltration.

Le *business model* du blanchisseur international est celui d'un opérateur de services évoluant dans un secteur concurrentiel. Les blanchisseurs sont constamment à la recherche de clients. Il est donc assez facile d'entrer en contact avec eux, soit à l'aveugle, soit de manière ciblée.

L'utilisation d'agents infiltrés donne des résultats probants. La méthode, ce n'est pas un secret, est utilisée par de nombreux pays, France, Pays-Bas et États-Unis en tête, qui possèdent une précieuse expérience en la matière. Ces techniques facilitent l'identification rapide des collecteurs. Ces petites mains du système jouent un rôle modeste mais leur identification permet de démarrer des enquêtes classiques sur les circuits de blanchiment : surveillances physiques et techniques, identification des clients et des commanditaires.

Ce type d'investigation, menée conjointement avec les divers pays affectés, a largement fait la preuve de son efficacité. De telles enquêtes ont permis d'alimenter les procédures judiciaires d'équipes communes dirigées contre les cartels de la drogue, de saisir des fonds considérables, d'identifier rapidement les réseaux de blanchiment, de démanteler l'infrastructure (comptes bancaires, sociétés), d'appréhender les équipes locales de trafiquants et de désorganiser les groupes criminels tout en recueillant des preuves irréfutables.

L'infiltration ouvre ainsi des perspectives immenses mais comporte évidemment des défis nécessitant une réactivité extrême et une grande agilité dans l'organisation de la coopération.

La méthode a démontré un exceptionnel retour sur investissement en permettant d'obtenir des résultats spectaculaires et de saisir de grandes quantités d'argent sans recourir à une débauche de moyens policiers. Les statistiques américaines disponibles parlent d'elles-mêmes, avec vingt ans de recul. Pour un dollar investi dans une opération de ce type, la DEA (Drug Enforcement Administration) en récupère cent sous forme de saisies des avoirs criminels… en plus des résultats judiciaires.

L'efficacité de la méthode contre ces réseaux internationaux est bien illustrée par une opération d'infiltration menée en France en collaboration avec la DEA américaine en 2015, débouchant sur de lourdes condamnations pour blanchiment du produit du trafic international de cocaïne.

Dans cette affaire, les trafiquants de cocaïne dissimulaient leurs opérations de blanchiment au moyen d'opérations commerciales. L'argent liquide était investi en marchandises en Europe, exportées en Afrique et au Moyen-Orient puis revendues. Cette méthode, rentable pour les blanchisseurs, est complexe à démontrer pour les enquêteurs. Les marchandises peuvent être acquises dans un autre pays que celui où elles sont prises en charge, les transactions paraissent légales et les acteurs sont nombreux… Or, cette enquête a révélé comment un réseau mondial

basé au Moyen- Orient et en Amérique du Sud blanchissait des dizaines de millions d'euros au profit de cartels colombiens et mexicains. Grâce aux moyens d'enquête spéciaux et à une coopération internationale intense, moins de deux mois ont été nécessaires pour identifier un réseau tentaculaire et planifier une opération simultanée dans sept pays. Tout ceci grâce à une simple remise de fonds initialement observée à Paris.

Aussi complexes et sophistiquées soient-elles, ces opérations de blanchiment liées au crime organisé découlent généralement d'une collecte initiale d'espèces, des mains des petits trafiquants, par des équipes dédiées.

C'est précisément à cette étape, la plus vulnérable du circuit, qu'il faut agir.

Notes :

1. Auteur avec la collaboration de Hélène CONSTANTY d' « Argent sale : la traque », aux éditions Fayard, 20 janvier 2021.

OUVRAGES RÉCENTS

DICTIONNAIRE DES MAFIAS ET DU CRIME ORGANISÉ

AUTEUR : PHILIPPE DI FOLCO

ÉDITEUR : PERRIN

Résumé

La mafia passée au crible de son histoire.

Philippe di Folco livre le premier dictionnaire consacré aux mafias et à leur univers tentaculaire.

Des *Big six* – constitués des mafias d'origine italienne, des groupes russes, des yakuzas, des triades chinoises, des cartels de la drogue colombien et des cartels mexicains – aux groupes émergeants (Argentine, Brésil, Jamaïque, Panama, Puerto Rico, République dominicaine, Sierra Leone), il étudie toutes les organisations criminelles sans exception, se penche

sur leur fonctionnement et leurs liens, leurs membres, leurs modes opératoires comme leur code de langage.

Figurent naturellement les notices biographiques de grands mafieux comme Al Capone, Lucky Luciano, Meyer Lansky ou Yosho Kodama mais d'autres aussi thématiques, telles que intimidation, cadavre, extorsion des fonds ou blanchiment de l'argent.

Un dictionnaire passionnant où les histoires se croisent et se lient pour dessiner une immense fresque des mafias et du crime organisé.

ÉTAT CIVIL, IDENTITÉ ET BIOMÉTRIE, EN PRATIQUE, QU'EST-CE QUE L'IDENTITÉ LÉGALE ?

MARIANNE BONDAZ

INSPECTRICE GÉNÉRALE DE L'ADMINISTRATION (IGA)

La définition de l'identité légale[1], au sens de l'identification d'une personne reste difficile à appréhender dans le droit français alors que cette notion commande l'exercice de nos droits et notre capacité d'aller et venir. La logique de l'identification est également inhérente à l'État parce qu'elle participe de la réalisation de sa souveraineté.

Certes le croisement des textes permet bien de relier les éléments constitutifs de l'identité à l'état civil. Mais l'état civil n'apparaît plus comme une donnée suffisante pour sécuriser l'identité. La correspondance entre l'identité biométrique d'un individu et le titre d'identité qu'il détient s'impose, face à la montée des fraudes documentaires et à l'identité, alors que le renforcement des dispositifs de sécurité physique des titres de voyage a mis en évidence la fragilité de l'état civil, soit parce que certains États ne sont pas en mesure d'en garantir la complétude et la fiabilité, soit parce que la fraude se porte sur les actes d'état civil, plus facilement falsifiables.

I. État civil, identité et identité biométrique

A. L'état civil est un droit, la preuve d'identité une nécessité

L'état civil est appréhendé comme un droit de l'individu conféré par l'autorité publique, alors que nos textes abordent la notion d'identité plutôt sous l'angle de sa preuve ou de ses conditions de vérification, voire de contrôle.

Si l'état civil ouvre droit à une capacité juridique définie dans le Code civil, l'identité est en revanche évoquée par les hypothèses où elle peut être vérifiée. On la retrouve dans la loi n°2012 -410 du 27 mars 2012 relative à la protection de l'identité et de nombreux Codes : Code des relations entre le public et l'administration (CRPA), Code général des impôts, Code des douanes, Code pénal, Code de procédure pénale, Code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA), Code électoral, notamment.

Identité et état civil sont indissociablement liés : une identité fiable ne peut reposer que sur un état civil bien organisé, reconnu et sûr ; un état civil doit pouvoir être attesté facilement dans la vie courante - pour voyager, pour faire valoir ses droits, obtenir des prestations, voter… - d'où l'importance des titres d'identité.

Au plan international, les considérations de droit privé et de droit public ne sont pas distinguées, l'identité d'une personne étant un droit d'autant plus précieux qu'il n'est pas partagé par tous comme l'explicite sur son site l'organisation non gouvernementale Humanium de protection des droits de l'enfant[2] :

« *Dès la naissance, chaque personne a le droit d'avoir une identité. L'identité d'une personne est l'affirmation de son existence au sein d'une société. C'est également la reconnaissance de son individualité et de ce qui la différencie de ses prochains. (…).*

Posséder une identité est un droit humain fondamental qui permet à chaque personne de pouvoir jouir de l'ensemble de ces droits.

L'identité regroupe le nom, le prénom, la date de naissance, le

sexe et la nationalité de la personne. Grâce à ces informations, une personne sera titulaire de droits et obligations spécifiques à son statut (femme, homme, enfant, handicapé, réfugié, etc.). »

B. L'identité « se prouve »

En France, l'état civil est un acquis, mais l'identité qui en découle « *se prouve* », « *par tous moyens* » et plus généralement par la détention d'un titre d'identité ou de voyage (TIV)[3].

C'est dans la définition des cartes nationales d'identité (CNI) ou des passeports que l'on retrouve les attributs de cette identité sans que celle-ci soit formellement définie :

« La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :

> *1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;*
>
> *2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;*
>
> *3° Son domicile ;*
>
> *4° Sa taille et la couleur de ses yeux ;*
>
> *5° Ses empreintes digitales ;*
>
> *6° Sa photographie. (…)* » (article 2 de la loi n° 2012-410 du 27 mars 2012)

Aux attributs d'état civil, absolument nécessaires pour définir l'identité et obtenir un TIV, s'ajoutent ainsi des caractéristiques biométriques qui ne figurent pas à l'état civil[4].

C. L'identité « se contrôle »

L'identité « se contrôle » de façon volontaire, par exemple aux frontières ou pour certains actes importants de la vie courante où l'identité doit être vérifiée. Elle peut aussi être contrôlée sous la contrainte, dans un cadre défini par le Code de procédure pénale (CPP).

En l'absence de justification d'identité ou en présence d'éléments d'identité manifestement inexacts, c'est bien sur les données biométriques de la personne qu'on va s'appuyer pour tenter de déterminer ses attributs d'état civil ou si elle est déjà « connue » pour d'autres infractions, y compris sous un autre nom (alias). L'identité est alors dissociée de l'état civil allégué qui peut être faux ou usurpé.

D. L'identité est l'objet de fraude

La fraude à l'identité, infraction en elle-même, est un vecteur d'immigration irrégulière, d'escroquerie ou, plus généralement, un moyen concourant à organiser une certaine impunité, voire évitant la qualification de récidive légale (usage d'alias).

L'Observatoire national de la délinquance et des réponses pénales (ONDRP) donne la définition suivante de la fraude documentaire et à l'identité :

« *La fraude aux documents et à l'identité regroupe deux types de fraudes bien distinctes dans leurs modes de réalisation : la fraude documentaire et la fraude à l'identité.*

> *1. La fraude documentaire porte principalement sur la falsification et la contrefaçon de documents (articles 441-1 et 441-2 du Code pénal).*
>
> *2. La fraude à l'identité ne se limite pas à la fraude documentaire, elle se traduit également par l'usurpation d'identité (articles 434-23 et 226-4-1 du Code pénal) et l'altération d'identité (article 433-19 du Code Pénal), la prise du nom d'un tiers (article 434-23 du Code pénal) et de l'obtention indue de documents (article*

Rappel des conditions de vérification d'identité sous le contrôle de l'autorité judiciaire (article 78 et suivants du CPP)

Pour toute personne à l'égard de laquelle existe une ou plusieurs raisons plausibles de soupçonner :
- qu'elle a commis ou tenté de commettre une infraction ;
- qu'elle se prépare à commettre un crime ou un délit ;
- qu'elle est susceptible de fournir des renseignements utiles à l'enquête en cas de crime ou de délit ;
- qu'elle a violé les obligations ou interdictions auxquelles elle est soumise dans le cadre d'un contrôle judiciaire (…) ;
- qu'elle fait l'objet de recherches ordonnées par une autorité judiciaire.

Ainsi qu'**à l'égard de ces personnes pour prévenir une atteinte à l'ordre public**, notamment à la sécurité des personnes ou des biens.

Sur réquisition écrite du procureur de la République aux fins de recherche et de poursuite d'infractions qu'il précise, l'identité de toute personne peut être également contrôlée, selon les mêmes modalités, dans les lieux et pour une période de temps déterminés par ce magistrat. Le fait que le contrôle d'identité révèle des infractions autres que celles visées dans les réquisitions du procureur de la République ne constitue pas une cause de nullité des procédures incidentes.

Dans une zone comprise entre la frontière terrestre de la France avec les États parties à la convention signée à Schengen le 19 juin 1990 et une ligne tracée à 20 kilomètres en deçà, ainsi que dans les zones accessibles au public des ports, aéroports et gares ferroviaires ou routières ouverts au trafic international et désignés par arrêté et aux abords de ces gares, pour la prévention et la recherche des infractions liées à la criminalité transfrontalière, l'identité de toute personne peut également être contrôlée, en vue de vérifier le respect des obligations de détention, de port et de présentation des titres et documents prévues par la loi (autres règles applicables outre-mer).

441-6 al.1 du Code pénal).

Ces délits sont par essence moins faciles à cerner, car ils sont généralement réalisés en support d'une autre infraction. En effet, ce type de fraude porte aussi bien sur les justificatifs nécessaires à l'obtention de titres (état civil) que sur les titres eux-mêmes. La fraude à l'identité recouvre deux grands types de modes opératoires :

1. L'usage frauduleux d'un document authentique : le fraudeur utilise un document authentique qui ne lui appartient pas et se sert de sa ressemblance physique avec le titulaire.

2. L'obtention indue de documents : le délinquant va présenter des faux justificatifs ou des justificatifs d'un tiers pour obtenir un document authentique. L'identité utilisée peut être celle du fraudeur, d'un tiers ou d'une identité fictive.[5]»

La typologie de fraude retenue pour mesurer le phénomène dans sa globalité au plan français et européen par la direction de la police aux frontières est la suivante :

Pour les usages de fausses identités les plus exigeants ne pouvant se limiter à l'usage de faux documents de plus en plus repérables avec le renforcement des sécurités physiques des TIV, la fraude s'oriente mondialement vers l'usage illégal de documents authentiques de voyage :

- soit par le recours à de faux documents d'état civil, l'obtention frauduleuse de vrais documents d'état civil ou à des documents d'état civil usurpés, plus facilement falsifiables ou « achetables », permettant la délivrance de vrai TIV ;

- soit par l'utilisation d'un vrai document d'identité par un tiers ressemblant (fraude dite au *look alike*), en connivence avec le titulaire du titre ou sans son accord[6] (réutilisation de titres perdus / volés) ;

- soit, pour parer les éventuels contrôles automatisés par le recours à des photographies « morphées »[7].

II. L'exigence croissante d'une vérification biométrique pour garantir l'identité

A. La vérification d'identité comporte de plus en plus souvent un volet biométrique

Afin de sécuriser le contrôle aux frontières, la production d'un document de voyage comportant les éléments d'état civil ne suffit plus en pratique ; encore convient-il de s'assurer que son détenteur en est bien le titulaire par vérification de la conformité des données biométriques relevées lors de la délivrance du titre avec celles du détenteur qui passe physiquement la frontière.

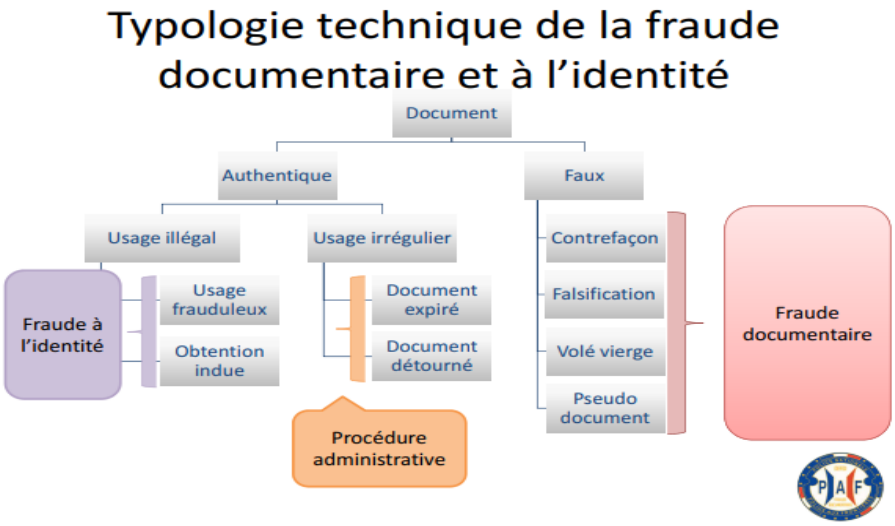
Cette vérification est de plus en plus souvent assistée par vérification automatisée de l'image faciale ou des empreintes digitales intégrées dans la puce du passeport (exemple des SAS PARAFE[8] dans nos aéroports à la gare du Nord pour les trains vers le Royaume-Uni).

Pour des déplacements internationaux, la production d'un simple document officiel physique ne suffit plus à garantir l'identité de façon totalement fiable. Cette évolution, initiée par l'Organisation de l'aviation civile internationale (OACI) est maintenant reprise en Europe notamment pour le contrôle de nos frontières, la lutte contre l'immigration irrégulière, mais également pour lutter contre la criminalité internationale et le terrorisme.

B. L'OACI a initié le développement de dispositifs biométriques incorporés dans les passeports

Le rôle de l'OACI s'ancre dans la Convention relative à l'aviation civile internationale (« Convention de Chicago » signée le 7 décembre 1944) qui couvre les conditions requises pour que les activités d'aviation civile soient efficaces et ordonnées, avec l'obligation incombant aux États d'adopter des procédures normalisées internationalement pour les formalités de douane et d'immigration (article 37, alinéa j).

Les normes de l'OACI ont pour



objectif de faciliter les formalités pour les voyageurs aériens, grâce à un niveau de confiance satisfaisant dans la fiabilité des documents de voyage.

La Convention de Chicago[9] distingue des normes obligatoires (les États contractants ne les respectant pas devant le déclarer à l'OACI) des pratiques recommandées. Ces règles structurent les conditions de validité des documents de voyage aux frontières. Les principales normes et recommandations portent notamment sur :

- la durée de validité du passeport dont la détention, éventuellement accompagnée par un visa, suffit à franchir les frontières (durée maximale recommandée de dix ans) ;

- les spécifications techniques des passeports qui comprennent une bande lisible à la machine (ou bande MRZ) et dont les sécurités doivent être régulièrement actualisées « *pour se prémunir contre leur usage indu et pour faciliter la détection de cas dans lesquels de tels documents ont été illicitement modifiés, reproduits ou délivrés* » ; il est par ailleurs recommandé que les passeports incorporent des données biométriques selon des normes communes[10] ;

- la lutte contre la fraude, les États devant fournir « *sans délai à INTERPOL des informations exactes relatives aux documents de voyage volés, perdus ou révoqués émis par leur pays, aux fins d'inclusion dans la base de données sur les documents de voyage volés ou perdus (SLTD)* » et établir des « *contrôles appropriés sur l'ensemble des processus de demande, d'octroi et de délivrance des documents de voyage pour garantir un niveau élevé d'intégrité et de sûreté* ».

Par ailleurs, plusieurs facteurs de sécurisation doivent être pris en considération dans le processus de demande, par exemple un examen plus minutieux en cas de première demande ou la comparution en personne devant un agent du gouvernement.

C. Les normes de sécurisation des titres européens ont été harmonisées et accrues

Dans un cadre de libre circulation des personnes, la lutte contre la falsification des documents de voyage devient une question d'intérêt commun au sein de l'Union européenne afin de faire face aux enjeux de criminalité organisée, d'immigration illégale et de terrorisme.

Ceci a conduit les États membres à mettre progressivement en place des règles communes de sécurisation des documents de voyage, dont le socle minimal est constitué par les normes OACI, afin de mieux protéger l'identité dans l'espace européen.

Les normes de sécurité des passeports et documents de voyage ont été précisées par le règlement CE 2252/2004 du Conseil du 13 décembre 2004 établissant des règles communes de sécurité matérielle et biométrique concernant les passeports et les documents de voyage délivrés par les États membres.

Les cartes nationales d'identité, bien que non obligatoires, devront également satisfaire à des normes communes puisqu'elles sont admises comme documents de voyage au sein de l'UE avec le règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation. La mise en oeuvre de ce règlement est échelonnée dans le temps[11]. Ces nouvelles cartes d'identité intègrent des données biométriques, empreintes digitales et photographies, dans un composant électronique hautement sécurisé.

Comme pour les passeports, il sera donc possible de renforcer la lutte contre la fraude documentaire et l'usurpation d'identité, en vérifiant la cohérence des données figurant sur le titre et celles figurant sur la puce. C'est donc une sécurité supplémentaire pour la nouvelle carte d'identité et son titulaire légitime.

Par ailleurs, les titres de séjour des étrangers (TSE) ainsi que les visas concernant les ressortissants des pays tiers sont normés afin d'assurer la libre circulation des étrangers autorisés à séjourner en France dans l'espace européen tout en sécurisant cet espace. L'intégration d'identificateurs biométriques dans les TSE est requise dans les modèles uniformes de titre de séjour : ils comportent une photo récente du demandeur et deux empreintes digitales[12]. Pour les visas de court séjour, le Code communautaire des visas[13] prévoit un enrôlement biométrique des demandeurs et leur enregistrement dans une base de données communautaire (cf. point 3 ci-après).

Ce contrôle fait de plus en plus appel aux composantes biométriques de l'identité pour éviter l'immigration irrégulière. Cette composante biométrique est d'autant plus nécessaire que de nombreux pays tiers ne disposent pas d'un état civil fiable ou de garanties relatives à la sécurisation du processus de délivrance de titres d'identité ou de voyage (état civil défaillant, phénomènes de corruption, défaillances du système de délivrance des documents de voyage).

Il convient enfin de noter qu'une demande d'asile n'est pas subordonnée à la production de documents d'état civil ou d'identité. Il est en effet tenu compte de la rupture du lien entre un demandeur d'asile et les autorités de son pays d'origine qui a pu l'empêcher d'obtenir des documents officiels. De ce fait, l'attribution d'une demande à un étranger se fait d'abord par la vérification des empreintes digitales, qui permet le cas échéant de repérer d'éventuels doublons de demandes en Europe ou une autre identité connue.

III. Une fiabilisation du contrôle aux frontières de l'Europe fondée sur des vérifications biométriques

La libre circulation au sein de l'espace européen a pour corollaire un contrôle renforcé et coordonné des frontières externes, notamment vis-à-vis des ressortissants de pays tiers (RPT) dont les titres de voyage peuvent être moins fiables que ceux des ressortissants européens dont les sécurités ont été harmonisées.

A. Un contrôle aux frontière renforcé des ressortissants des pays tiers (RPT)

Ce contrôle renforcé induira à l'horizon 2022 une utilisation généralisée de la biométrie pour détecter des identités multiples éventuelles, alléguées par des ressortissants de pays tiers, grâce à la mise en place de nouveaux systèmes d'information et à leur interopérabilité.

Plusieurs systèmes d'information européens existent déjà afin de détecter à l'échelle européenne des identités multiples à l'aide de données biométriques :

- **le système d'information sur les visas (VIS)** permet d'enregistrer les personnes qui demandent un visa pour entrer dans l'espace Schengen et de procéder à des vérifications à leur sujet. Les autorités peuvent utiliser le VIS pour établir des correspondances biométriques afin d'identifier des personnes et prévenir le vol ou l'usurpation d'identité ; ce fichier comporte les photographies et les empreintes digitales des demandeurs ;

- **la base de données Eurodac** (European Dactyloscopy) comporte les empreintes digitales des demandeurs d'asile ou de protection subsidiaire qui ont été enregistrés dans les États membres de l'UE et les pays associés. Cette base de données permet de vérifier si un demandeur a déjà demandé l'asile dans un autre État membre, s'il a déjà été appréhendé au moment de son entrée illicite sur le territoire européen et de déterminer quel État membre est responsable de l'examen de sa demande.

La création prochaine d'un **système d'entrée/de sortie (EES - Entry-Exit System)** entraînera l'enrôlement des données des ressortissants de pays tiers (RPT) qui entrent dans l'espace Schengen, permettra de tracer les entrées, les sorties et les refus de l'espace Schengen, y compris pour les RPT n'étant pas soumis à visa. Ce système permettra également d'alerter les autorités compétentes en cas de dépassement de la durée de séjour autorisée (que les RPT soient soumis ou non à visa) et de s'affranchir du compostage du passeport lors du passage par un point de passage frontalier. Les données enregistrées seront les données biographiques et biométriques (empreintes digitales et image faciale).

B. Un cadre d'interopérabilité entre les fichiers européens relatifs à l'immigration et la coopération policière et judiciaire

Deux règlements européens du 20 mai 2019[14] créent un cadre d'interopérabilité entre les fichiers européens relatifs à l'immigration et à la coopération policière et judiciaire.

Cette interopérabilité concerne plusieurs systèmes d'information européens existants ou à créer : le système d'entrée/de sortie (EES), le système d'information sur les visas (VIS), le futur système européen d'information et d'autorisation concernant les voyages (ETIAS)[15], Eurodac, le système d'information Schengen (SIS) et le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN[16]).

Selon le Conseil de l'UE, « *L'interopérabilité des systèmes d'information permettra aux systèmes de se compléter et contribuera à faciliter l'identification correcte des personnes ainsi qu'à lutter contre*

la fraude à l'identité. Les éléments d'interopérabilité mis en place par les règlements sont les suivants :

- un portail de recherche européen permettant aux autorités compétentes d'effectuer des recherches en parallèle dans de multiples systèmes d'information, en utilisant les données tant biographiques que biométriques ;

- un service partagé de mise en correspondance de données biométriques permettant de rechercher et de comparer des données biométriques (empreintes digitales et images faciales) issues de plusieurs systèmes ;

- un répertoire commun de données d'identité, qui contiendrait les données biographiques et biométriques des ressortissants de pays tiers disponibles dans plusieurs systèmes d'information de l'UE ;

- un détecteur d'identités multiples chargé de vérifier si les données d'identité biographiques issues de la recherche existent dans d'autres systèmes couverts, afin de permettre de détecter les identités multiples liées au même ensemble de données biométriques. »[17].

En conclusion, après nous être posé la question du droit à l'état civil, avoir constaté son caractère nécessaire mais non suffisant pour prouver son identité en toutes circonstances, nous en arrivons à la capacité ouverte à une personne d'attester de son état civil, grâce à ses caractéristiques biométriques, par une forme de raisonnement circulaire.

C'est ainsi le cas des Français qui perdent leur passeport à l'étranger et qui peuvent grâce à leurs empreintes digitales prouver qu'ils sont bien les légitimes détenteurs du titre déclaré perdu/volé, ce qui facilite son renouvellement[18]. C'est également le cas des demandeurs d'asile qui peuvent, même en l'absence de tout document d'état civil ou d'identité, introduire une demande d'asile, en prouvant simplement grâce à leur relevé biométrique qu'ils ne sont pas connus sous un autre nom ou pour une autre demande d'asile en Europe. À terme, la vérification de certains éléments biométriques, par exemple contenus dans la puce du titre d'identité, sera peut-être nécessaire pour prouver son identité à distance alors que les téléprocédures concernent des démarches de plus en plus sensibles, nécessitant une identification forte.

Notes :

1. Le présent article ne portera pas sur l'identité numérique qui nécessiterait de trop grands développements particuliers.
2. https://www.humanium.org/fr/comprendre-droits-enfant/droit-a-l-identite/
3. Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, article 12 « L'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier. »
4. Cf. article 4 du décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité et article 5 du décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports qui rendent nécessaire la production d'un « extrait d'acte de naissance de moins de trois mois, comportant l'indication de sa filiation ou, lorsque cet extrait ne peut pas être produit, de la copie intégrale de son acte de mariage. » pour toute première demande.
5. Éléments de connaissance sur la fraude aux documents et à l'identité en 2016 - ONDRP – https://www.ihemi.fr/sites/default/files/publications/files/2019-12/note_16.pdf
6. L'OCRIEST fait état de filières de revente des documents d'identité ou voyage Français, y compris à l'étranger. Voir par exemple https://www.francetvinfo.fr/france/que-deviennent-les-papiers-d-identite-voles_153135.html ou https://www.leparisien.fr/faits-divers/les-passeports-voles-a-barbes-etaient-vendus-aux-migrants-en-turquie-et-en-grece-26-07-2019-8124441.php
7. Morphose : technique consistant à leurrer un contrôle en mélangeant les caractéristiques des visages de deux personnes sur une photographie d'identité.
8. Passage rapide aux frontières extérieures (PARAFE)–https://www.immigration.interieur.gouv.fr/Europe-et-International/La-circulation-transfrontiere/Le-passage-rapide-aux-frontieres-exterieures-PARAFE
9. Annexe 9 à la Convention de Chicago - Facilitation - Quinzième édition, octobre 2017 https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons_fr.pdf Les citations qui apparaissent dans les paragraphes qui suivent viennent de ce document.
10. *« Il est recommandé que les États contractants incorporent des données biométriques dans leurs documents de voyage lisibles à la machine, dans un circuit intégré (puce électronique) sans contact, comme il est indiqué dans le Doc9303 – Documents lisibles à la machine »* Annexe 9 à la Convention de Chicago.
11. À compter du 2 août 2021, tout usager souhaitant se voir délivrer une carte nationale d'identité (CNI) ou souhaitant faire renouveler sa CNI arrivée à expiration, bénéficiera de la nouvelle carte. https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2021-06//brochure-carte-identite.pdf
12. Règlement (CE) no 1030/2002 — modèle uniforme de titre de séjour pour les ressortissants de pays non membres de l'UE. Le règlement (CE) no 380/2008 modifie le règlement (CE) no 1030/2002 en ce qui concerne l'intégration d'identificateurs biométriques dans les modèles uniformes de titre de séjour. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33043
13. Règlement (CE) N°810/2009 du Parlement européen et du Conseil du 13 juillet 2009 et notamment article 13 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32009R0810&from=EL
14. Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas C : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32019R0817 Règlement (UE) 2019/818 du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32019R0818
15. European Travel Information and Authorization System dont la création est prévue en 2022 et qui sera utilisé pour effectuer des vérifications en amont en ce qui concerne les voyageurs des pays tiers exemptés de visa, auxquels une autorisation de voyage pourra être refusée (système comparable aux systèmes déjà en place aux États-Unis, au Canada et en Australie).

16. *European Criminal Records Information System for third country nationals and stateless persons.* Ce traitement permet aux magistrats d'un État membre de déterminer si un ressortissant d'un pays tiers a été condamné dans un ou plusieurs États membres de l'Union Européenne. Pour chaque RPT, l'autorité centrale de l'État membre de condamnation crée un enregistrement de données dans le système central d'ECRIS-TCN qui contient des données biographiques, dactyloscopiques (empreintes) et faciales (photo numérisée).

17. Site du Conseil de l'UE – communiqué de presse en date du 5 février 2019 C : https://www.consilium.europa.eu/fr/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement

18. Cf. procédure à l'étranger : https://www.service-public.fr/particuliers/vosdroits/F34478/1_0_1_1_0?idFicheParent=N360#1_0_1_1_0

OUVRAGES RÉCENTS

PRÉCIS DE DROIT PÉNAL FISCAL

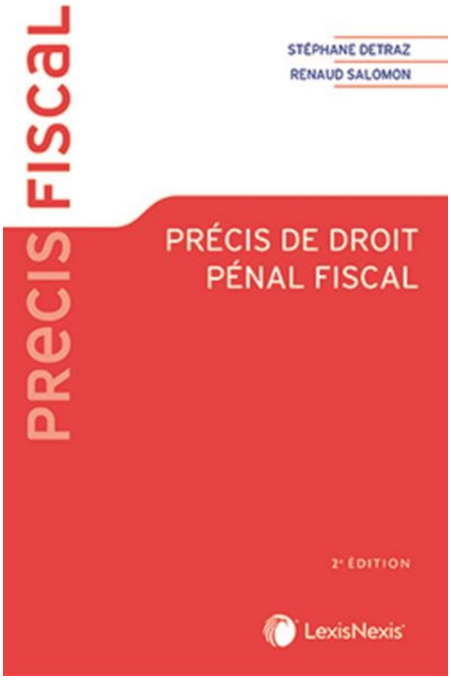
AUTEURS : STÉPHANE DETRAZ ET RENAUD SALOMON

ÉDITEUR : LEXISNEXIS

Résumé

Le droit pénal fiscal est la branche du droit criminel qui prévoit la répression des diverses formes de soustraction à l'impôt, en ses versants substantiel (incriminations, responsabilité pénale, sanctions) et procédural (phase administrative, enquête, poursuites, instruction, jugement). Le présent ouvrage examine en détail chacun de ces aspects, l'accent étant mis sur les deux infractions majeures que sont le délit général de fraude fiscale et le délit comptable. De longs développements sont également consacrés aux infractions voisines : escroquerie à la TVA, blanchiment et recel consécutifs à la fraude fiscale, etc.

La matière, longtemps assoupie, connaît depuis le début des années 2010 de profondes mutations de la part du législateur et de la jurisprudence. Ces évolutions procèdent de deux objectifs éventuellement antagonistes : d'une part, améliorer et renforcer la répression pénale de la fraude fiscale, notamment par l'alourdissement des peines et l'allégement des formalités préalables aux poursuites ; d'autre part, subordonner cette répression aux décisions de l'Administration fiscale et du juge de l'impôt, le recouvrement de la créance fiscale étant en ligne de mire. L'articulation entre la procédure pénale et la procédure fiscale, l'autorité judiciaire et l'autorité administrative, le juge pénal et le juge administratif en est rendue plus complexe encore.



Ce précis est à jour des nouveautés législatives et jurisprudentielles les plus récentes. Il s'adresse aux étudiants de master, aux universitaires ainsi qu'aux praticiens du droit (magistrats, avocats, notaires, etc.) et, plus largement, aux professionnels des secteurs financier, comptable et économique (banquiers, commissaires aux comptes, experts-comptables, chefs d'entreprise, etc.) intéressés par la matière fiscale.

Stéphane Detraz est maître de conférences HDR à l'université Paris-Saclay où il co-dirige le master II Droit pénal fondamental et pratique du droit pénal. Il est titulaire ou co-titulaire de plusieurs chroniques de jurisprudence, dont la chronique annuelle de droit pénal fiscal et douanier publiée à la revue Droit pénal, aux éditions LexisNexis.

Renaud Salomon est avocat général à la chambre criminelle de la Cour de cassation. Professeur associé à l'université de Paris Dauphine PSL, il est co-auteur de plusieurs ouvrages en droit pénal de l'entreprise (droit pénal des affaires, droit pénal du travail et de la sécurité sociale, droit pénal des marchés financiers, droit pénal comptable) et titulaire de diverses chroniques, dont la chronique trimestrielle de droit pénal fiscal, publiée à la revue Droit fiscal, aux éditions LexisNexis.

LA LOI SAPIN II À L'ÉPREUVE DE L'INTERNATIONAL

VÉRONIQUE BRUNEAU BAYARD

AVOCATE AU BARREAU DES HAUTS-DE-SEINE,
CMS FRANCIS LEFEBVRE AVOCATS

Pendant de nombreuses années, comparée à d'autres pays, la France était considérée, notamment par l'Organisation de Coopération et de Développement Économiques (OCDE), comme n'étant pas suffisamment impliquée dans la lutte contre la corruption. Ce, jusqu'en décembre 2016, lorsqu'une loi a imposé aux sociétés répondant à certains critères de mettre en place un programme de lutte contre la corruption et le trafic d'influence. Ainsi, l'article 17 de la loi du 9 décembre 2016[1] relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (la « Loi Sapin 2 »), a imposé aux sociétés ayant au moins 500 salariés et comptabilisant un chiffre d'affaires supérieur à 100 millions d'euros, de mettre en place un programme de lutte contre la corruption et le trafic d'influence composé de précisément huit mesures. Cette obligation concerne l'ensemble des sociétés ayant leur siège social en France y compris les filiales de sociétés étrangères remplissant ces deux critères. Si dans les pays anglo-saxons la mise en place de mesures anticorruption est solidement ancrée depuis longtemps dans la culture des sociétés, en France, avant décembre 2016, seules quelques sociétés avaient mis en place un dispositif de prévention de la corruption. Il s'agissait, par exemple, de sociétés cotées françaises, notamment des groupes du CAC40, de sociétés ayant une forte activité à l'international ou de sociétés cotées aux États-Unis. À la suite notamment des lourdes amendes prononcées par les autorités américaines contre des groupes européens, plusieurs sociétés s'étaient cependant dotées d'un programme anticorruption efficace afin d'éviter des sanctions financières et se voir imposer la mise en place d'un programme de compliance sous contrainte comme peut l'exiger l'autorité américaine. Aujourd'hui, la compliance est devenue un sujet majeur pour l'ensemble des acteurs économiques et en renforçant en 2016 son dispositif anticorruption, la France s'est alignée sur les standards internationaux les plus exigeants.

I. L'exigence française d'un programme anticorruption précis

Contrairement à la France, aux États-Unis par exemple, il n'existe pas d'obligation légale pour les sociétés de mettre en place un programme anticorruption. C'est seulement dans le cas d'une suspicion de corruption que le département de la justice américain examinera l'efficacité du programme anticorruption mis en place par la société. Si les pays anglo-saxons privilégient une approche plus générale, l'article 17 de la loi Sapin 2 prévoit lui spécifiquement les huit mesures[2] que les sociétés doivent obligatoirement mettre en place. Cette loi a également créé une agence dédiée à la prévention et la détection des faits de corruption et de trafic d'influence : l'Agence Française

Anticorruption (AFA) qui exerce à la fois des missions de conseil, d'assistance et de contrôle. L'AFA a élaboré plusieurs recommandations et guides pratiques qui, avec la loi Sapin 2 et ses décrets d'application, constituent le référentiel anticorruption français. C'est donc elle qui contrôle la réalité et l'efficience des mécanismes anticorruption des sociétés. Le défaut de mise en oeuvre d'un dispositif anticorruption par les sociétés qui y sont contraintes est sanctionné par une injonction de se mettre en conformité et par des amendes qui s'appliquent à la société comme aux dirigeants.

L'obligation pour les sociétés françaises de mettre en place un programme de lutte contre la corruption a entraîné une réelle prise de conscience des dirigeants quant à l'importance de ce sujet. L'obligation de réaliser une cartographie des risques de corruption et de trafic d'influence a conduit les entreprises à s'interroger, identifier, analyser et hiérarchiser leurs risques de corruption et donc à mener en interne une véritable réflexion sur ce sujet. Il leur est également apparu nécessaire de développer, au sein de la société ou du groupe, en France comme à l'étranger, une véritable culture éthique. L'élaboration puis la diffusion du code de conduite à l'ensemble des salariés ainsi que la mise en place de formations pour les dirigeants et le personnel le plus exposé, ce afin de répondre aux exigences de la loi Sapin 2, ont également contribué à cette nécessaire prise de conscience. En effet, en matière de lutte contre la corruption, il est indispensable que l'impulsion vienne du plus haut de l'exécutif "*tone from the top*" afin d'inculquer, de développer et de promouvoir une véritable culture éthique dans la société ou le groupe. On associe souvent gouvernance et compliance car, il est vrai qu'au-delà du respect des normes juridiques impératives, il convient que l'ensemble des acteurs de l'entreprise s'impliquent et que le « top management » bénéficie d'un support actif du conseil d'administration afin que la compliance se retrouve véritablement dans l'ADN de la société.

Au-delà de la mise en oeuvre opérationnelle du programme anticorruption, il convient de promouvoir et de diffuser une véritable culture éthique dans l'ensemble des filiales du groupe, y compris et surtout, dans les filiales étrangères. En effet, ces dernières sont souvent éloignées des centres de décision et il est important qu'elles se sentent concernées par la politique compliance du groupe. L'efficacité d'un programme anticorruption implique qu'il soit connu, compris et appliqué sur le terrain. Il est donc indispensable d'établir des relais dans les filiales avec un référent local, le *compliance officer*, pour développer une véritable politique anticorruption au sein du groupe. Compte tenu des enjeux importants que représente la corruption, non seulement en termes financiers mais également en termes d'image ou de réputation, les sociétés ont compris qu'il était nécessaire d'accorder des moyens matériels et humains importants afin de mettre en place les outils appropriés à la réalisation d'un programme compliance efficace. Généralement, celui-ci ne se limite pas à la prévention et à la lutte contre la corruption mais comprend d'autres domaines liés à la compliance comme la lutte contre le blanchiment d'argent et le financement du terrorisme, la prévention des conflits d'intérêts[3], la gestion de l'information privilégiée ou les délits d'initiés dans le cas de sociétés cotées.

II. Corruption et extraterritorialité

La loi Sapin 2 a été élaborée avec un double objectif : répondre au renforcement des réglementations internationales dans le domaine de la lutte contre la corruption mais également concurrencer l'action des autorités étrangères. En effet, cette loi tend à s'aligner sur certains textes d'application extraterritoriale qui ont contraint les entreprises françaises à prendre les mesures nécessaires pour se conformer à leurs dispositions. Ainsi, aux États-Unis, le *Foreign Corrupt Practices Act* (FCPA), s'applique à toutes les entreprises enregistrées ou cotées sur une bourse américaine, quel que soit leur lieu d'incorporation, à toutes les personnes physiques ou morales américaines, ainsi qu'à certaines personnes ou entités exerçant une activité aux États-Unis. Au Royaume-Uni, c'est le *UK Bribery Act* (UKBA), qui s'applique aux délits commis dans le monde entier par des ressortissants britanniques, aux sociétés immatriculées en Angleterre, ainsi qu'à toute personne conduisant des affaires en Angleterre et ce quel que soit son pays de constitution. Cependant, la mise en place en France de procédures destinées à prévenir la corruption ne permet pas de garantir que les autorités étrangères telles que le *Department of Justice* (DOJ) aux États-Unis ou le *Serious Fraud Office* (SFO) au Royaume-Uni ne

poursuivront pas des entreprises soumises au contrôle de l'AFA pour les mêmes faits, dès lors qu'aujourd'hui aucun texte n'interdit à une autorité étrangère de se saisir de faits pour lesquels elle s'estimerait compétente. Il est donc difficile de savoir si la loi Sapin 2 permettra aux entreprises françaises de ne plus subir l'extraterritorialité américaine ou britannique. L'extraterritorialité du droit américain permet en effet aux États-Unis de poursuivre les entreprises françaises pour des faits commis en dehors du territoire américain lorsqu'il existe un lien avec les États-Unis, comme un paiement en dollars.

III. Règlement concerté des litiges et lutte internationale contre la corruption

La loi Sapin 2 a également créé une procédure permettant au procureur de la République de conclure une Convention Judiciaire d'Intérêt Public (CJIP) avec une personne morale mise en cause pour des faits d'atteintes à la probité. Cette mesure qui constitue une alternative aux poursuites est applicable aux entreprises, associations, collectivités territoriales, etc. poursuivies pour des faits de corruption, trafic d'influence, fraude fiscale, blanchiment de fraude fiscale et toute infraction connexe. Elle a pour effet d'éteindre l'action publique si la personne morale concernée exécute les obligations auxquelles elle s'est engagée dans la convention : (i) versement d'une amende d'intérêt public à l'État, (ii) mise en oeuvre, sous le contrôle de l'AFA, d'un programme de mise en conformité des procédures de prévention et de lutte contre la corruption pour une durée maximale de 3 ans et (iii) réparation du dommage de la victime. La CJIP est proposée par le procureur de la République et acceptée par la personne morale, elle doit ensuite faire l'objet d'une validation par le juge lors d'une audience publique. La convention et la décision de validation sont publiées sur le site internet de l'AFA.

La CJIP est inspirée des procédures de transactions pénales qui existent depuis de nombreuses années dans les pays anglo-saxons. Elle permet de régler des faits de corruption transnationale et de favoriser un règlement concerté des litiges alors que ces dernières années les procédures judiciaires extraterritoriales mettant en cause des sociétés françaises se sont multipliées. La CJIP permet également de régler plus rapidement les dossiers complexes. Depuis sa création et la première CJIP signée en octobre 2017, plus d'une douzaine de conventions ont été conclues et deux d'entre elles ont également donné lieu à un règlement simultané entre les autorités françaises et étrangères comme dans le cas de la Société Générale ou d'Airbus. Ainsi, la Société Générale a conclu une CJIP[4] le 24 mai 2018 qui a fait l'objet d'une ordonnance de validation par la cour d'appel de Paris le 4 juin 2018. Selon les termes de cette CJIP, la Société Générale s'est engagée à verser au Trésor public la somme totale de 250.150.755 euros et à faire évaluer par l'AFA, pendant 2 ans, la qualité et l'effectivité des mesures de prévention de la corruption qu'elle a mises en oeuvre depuis 2014. Sous réserve de l'exécution de ces obligations, la décision de validation acte la fin des poursuites engagées contre la Société Générale dans le cadre de l'enquête préliminaire ouverte le 18 novembre 2016 par le Parquet National Financier (PNF) du chef de corruption d'agents publics étrangers et qui concernait les relations d'affaires nouées entre la Société Générale et la *Libyan Investment Authority* au cours de la période 2007-2010. Ces faits ont également fait l'objet d'une enquête menée par le *Department of Justice* des États-Unis et le procureur fédéral du district-est de New York. Les autorités françaises et américaines ont coordonné leurs actions afin de parvenir à la signature simultanée avec la Société Générale d'une CJIP en France et d'un *Deferred Prosecution Agreement* (DPA) aux États-Unis, qui est un accord de suspension de poursuites. Cet accord prévoit que la banque versera la même somme de 250.150.755 euros au Trésor des États-Unis, sous réserve de validation du DPA par un juge fédéral. Comme l'indiquait le ministère de la Justice dans un communiqué de presse en date du 4 juin 2018, ce premier accord de résolution coordonnée constitue un progrès significatif dans la lutte contre la corruption internationale. La création de la CJIP a donc permis au Parquet National Financier de se positionner sur la scène internationale et de faire reconnaître l'efficacité du dispositif français de lutte contre la corruption. Cela a également permis une meilleure coopération entre les différents parquets et les sociétés ainsi que le versement d'amendes importantes au profit du Trésor public.

En 2020, une nouvelle avancée dans la lutte contre la corruption

internationale est intervenue dans le cadre du dossier Airbus qui a conduit à la signature simultanée de trois accords en France, au Royaume-Uni et aux États-Unis. Ainsi, le 31 janvier 2020, le président du tribunal judiciaire de Paris a validé la CJIP conclue le 29 janvier 2020 par le procureur de la République financier (PRF) et Airbus. Cette dernière s'est engagée à verser au Trésor public une amende d'intérêt public de 2.083.137.455 euros et à faire évaluer par l'AFA, pendant trois ans, l'effectivité de son programme de conformité, dont le contrôle diligenté par l'AFA en 2017 avait permis de constater qu'il était déjà abouti. Cette CJIP acte la fin des poursuites engagées contre Airbus dans le cadre de l'enquête préliminaire qui avait été ouverte le 20 juillet 2016 par le Parquet National Financier (PNF) et confiée à l'Office Central de Lutte contre la Corruption et les Infractions Financières et Fiscales (OCLCIFF). Leurs investigations ont porté sur des faits de corruption d'agents publics étrangers et de corruption privée commis entre 2004 et 2016, à l'occasion de contrats de vente d'avions civils et de satellites conclus par des entités du groupe Airbus. Ces investigations ont été conduites dans le cadre d'une équipe commune d'enquête constituée entre le PNF et le *Serious Fraud Office* (SFO) britannique et parallèlement à l'enquête ouverte par le *Department of Justice* des États-Unis et le procureur fédéral du district de Columbia (Washington DC). Le PNF, le SFO et les autorités judiciaires américaines ont coordonné leurs actions afin de parvenir à la signature simultanée d'une CJIP et de deux *Deferred Prosecution Agreements* avec Airbus. Les accords conclus séparément par Airbus avec le SFO et les autorités judiciaires américaines prévoient qu'Airbus versera une amende de 983.974.311 euros aux autorités britanniques et une amende de 525.655.000 euros au Trésor des États-Unis.

IV. Première évaluation de la Loi Sapin 2

Quatre ans après sa promulgation, la Loi Sapin 2 a fait l'objet d'une première évaluation. Ainsi, en décembre 2020, la Commission des lois de l'Assemblée nationale a confié aux députés Raphaël Gauvain[5] et Olivier Marleix[6] une mission d'évaluation de la loi Sapin 2, qui a donné lieu à un rapport[7], rendu le 7 juillet 2021. Cette mission intervient dans le double contexte de la transposition de la directive européenne du 23 octobre 2019 sur les lanceurs d'alerte[8], que la France doit transposer d'ici fin 2021, et de l'évaluation par l'OCDE de sa stratégie anticorruption. Il s'avère que les résultats de notre pays en matière de lutte contre la corruption stagnent puisque la France reste à la 23èmc place du classement de *Transparency International* sur la perception de la corruption, soit la même place qu'en 2015 avant la promulgation et la mise en place de la Loi Sapin 2. Les rapporteurs ont procédé à une évaluation approfondie des avancées portées par la loi Sapin 2 et ont formulé 50 propositions pour donner un nouveau souffle à la politique de lutte contre la corruption en France.

Il en résulte que la CJIP, inspirée des procédures de transactions pénales qui existaient déjà en droit anglo-saxon et créée par la Loi Sapin 2, a connu un véritable succès à la fois en favorisant un règlement concerté des litiges et également en conduisant à une véritable coopération avec les autorités étrangères. La CJIP offre un dispositif relativement souple qui permet aux parquets de disposer d'une grande marge de manoeuvre lors de sa mise en oeuvre et qui permet également une grande liberté pour les parties lors de sa négociation. La contrepartie de cette souplesse sont les faibles garanties accordées aux sociétés lors de la négociation de la CJIP, ce qui ne favorise pas vraiment une révélation spontanée des faits de leur part. Ainsi, lors d'une négociation, la société ne peut avoir la certitude que le parquet lui proposera de conclure une CJIP, ni connaître le montant de l'amende à laquelle elle s'expose. De plus, en cas d'échec des négociations, les informations et les documents qu'elle aurait éventuellement transmis au parquet pourraient être utilisés dans le cadre d'une procédure judiciaire. Compte tenu de ces incertitudes, il est difficile pour une société d'évaluer les avantages dont elle bénéficiera en concluant une CJIP par rapport aux risques encourus lors de la négociation, particulièrement dans le cas de la révélation de faits de corruption. Afin de permettre aux entreprises d'avoir une meilleure visibilité sur les bénéfices d'une négociation, les rapporteurs proposent de donner à la société l'assurance qu'elle pourra bénéficier d'une CJIP à certaines conditions notamment dans le cadre de sa pleine coopération lors d'une enquête[9]. De même, le dispositif français ne permet pas à la société d'estimer,

même approximativement, le montant de l'amende qui pourrait lui être infligée[10].

Le rapport s'est également intéressé au périmètre d'application de la loi Sapin 2 qui actuellement contraint les sociétés ayant au moins 500 salariés et dont le chiffre d'affaires est supérieur à 100 millions d'euros à mettre en place des mesures anticorruption dans la société elle-même ainsi que dans l'ensemble de ses filiales ou des sociétés qu'elle contrôle. Le rapport indique que le projet de loi Sapin 2 ne comportait pas d'explications sur le niveau de ces seuils, indiquant simplement que ces obligations devaient s'appliquer aux « plus grandes entreprises ». Lors de leur audition, certains ont relevé que ces seuils ne prenaient pas en compte le profil de risque de l'entreprise, qui dépend de nombreux paramètres, tels que le secteur d'activité, sa gouvernance, son implantation géographique, son organisation, son modèle économique ou encore l'identité des tiers. Interrogée sur ce sujet, l'AFA a reconnu que la fixation de seuils était difficile mais que les sociétés ou groupes français les plus importants devaient mettre en place un dispositif anticorruption. Comme ce dispositif implique notamment une évaluation des tiers cela conduit les entreprises qui travaillent avec ces sociétés ou ces groupes à mettre en place des mesures appropriées afin de leur montrer leur intégrité.

L'AFA a souligné que les groupes étrangers disposant de filiales en France qui ne dépassent pas les seuils précédemment mentionnés ne sont pas concernés par ces obligations. Ainsi, la condition d'établissement du siège de la société mère en France a pour effet d'exclure du périmètre de l'article 17 les groupes étrangers qui ne disposent pas sur le territoire national de filiales atteignant les seuils ou qui pourraient être tentés de réduire leurs effectifs pour ne pas être dans le périmètre de l'article 17[11]. Afin de remédier à cette situation, les rapporteurs ont proposé de supprimer la condition d'établissement du siège social de la société mère en France pour les filiales situées en France. Ils considèrent que cette suppression permettrait de rétablir une égalité de traitement entre les petites filiales de grands groupes situées en France, selon que la société mère est établie en France ou à l'étranger[12].

Les rapporteurs soulignent également que le bilan de l'application extraterritoriale de la loi Sapin 2 et, notamment, la poursuite de faits de corruption d'agents publics étrangers par des entreprises de nationalité étrangère exerçant une partie de leur activité en France est inexistant. Il existe différents modes de signalement mis à la disposition de l'autorité judiciaire afin de lui permettre d'apprécier l'opportunité d'ouvrir des enquêtes : l'administration fiscale, l'AFA, l'Autorité de la concurrence, l'Autorité des marchés financiers, certains opérateurs publics ou parapublics comme l'Agence française de développement et Bpifrance, la cellule de renseignement financier Tracfin, etc. Il y a donc de nombreux acteurs susceptibles d'apporter leur concours à la détection de faits de corruption internationale mais peu ont usé de cette possibilité et peu d'entreprises étrangères ont été poursuivies en France pour des faits de corruption commis à l'étranger. Les rapporteurs ont indiqué que les entreprises françaises implantées à l'étranger, dans des pays où la corruption est présente, sont parfois réticentes à l'idée de dénoncer ces faits aux parquets étrangers ou aux autorités locales par peur de répercussions sur leur accès à la commande publique ou de mesures de rétorsion. Par ailleurs, les services économiques des ambassades de France ne contribuent pas non plus à la dénonciation de faits de corruption. Tout d'abord car les informations qui leur sont transmises doivent être vérifiées, ce qui nécessite d'y affecter des moyens spécifiques, et d'autre part car une approche « offensive » de la lutte contre la corruption transnationale pourrait être mal perçue et avoir des effets négatifs sur l'attractivité de l'économie française que s'attachent à promouvoir les services économiques. Selon les rapporteurs, il est donc nécessaire de renforcer les moyens de détection des faits de corruption commis à l'étranger, en mobilisant plus fortement les différents services de l'État, ce qui est le sens de leur quatorzième proposition[13].

La Loi Sapin 2 a indéniablement marqué un tournant dans la lutte contre la corruption en France et a entraîné une véritable prise de conscience de la part des différents acteurs économiques. Les propositions formulées à la suite de la première évaluation de cette loi ainsi que la prochaine transposition de la directive européenne sur les lanceurs d'alerte constitueront indéniablement en France un nouveau

tournant et un renforcement des mesures anticorruption.

Notes :

1. Loi n° 2016-1691 du 9 décembre 2016.
2. (i) un code de conduite, (ii) un dispositif d'alerte interne, (iii) une cartographie des risques, (iv) des procédures d'évaluation de la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques, (v) des procédures de contrôles comptables, internes ou externes, destinées à s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de corruption ou de trafic d'influence, (vi) un dispositif de formation destiné aux cadres et aux personnels les plus exposés aux risques de corruption et de trafic d'influence, (vii) un régime disciplinaire permettant de sanctionner les salariés de la société en cas de violation du code de conduite et (viii) un dispositif de contrôle et d'évaluation interne des mesures mises en oeuvre.
3. Le 1er septembre 2021, l'AFA a publié un projet de guide pratique "Les conflits d'intérêts dans l'entreprise" afin de sensibiliser à la nécessité de mieux appréhender et gérer les risques de conflits d'intérêts dans l'entreprise. Ce guide, qui a été soumis à une consultation publique jusqu'au 30 septembre 2021, a vocation à accompagner les entreprises, leurs dirigeants ainsi que les professionnels de la conformité dans l'identification des situations à risque et dans la définition de mesures permettant de les prévenir et de les gérer.
4. Avec le procureur de la République financier près le tribunal de grande instance de Paris.
5. La République En Marche (LREM), Saône-et-Loire.
6. Les Républicains (LR), Eure-et-Loir.
7. Rapport d'information par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République en conclusion des travaux d'une mission d'information sur l'évaluation de l'impact de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin 2 » et présenté par MM. Raphaël Gauvain et Olivier Marleix, rapporteurs, députés.
8. Directive (UE) 2019/1937 du parlement européen et du conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.
9. Proposition n°20 : donner l'assurance à la personne morale qu'une CJIP lui sera proposée à certaines conditions (notamment, si elle coopère pleinement).
10. Proposition n°21 : prendre en compte la pleine coopération de l'entreprise, et notamment la révélation spontanée des faits de corruption, par la minoration de l'amende, selon un barème public.
11. L'AFA a indiqué souhaiter « ouvrir un nombre significatif de contrôles sur des filiales françaises de groupes étrangers ».
12. Proposition n° 1 : Supprimer la condition tenant à la localisation en France du siège social de la société mère, afin de soumettre aux obligations prévues par l'article 17 les petites filiales de grands groupes étrangers établies en France, dès lors que la société mère dépasse les seuils prévus par la loi.
13. Proposition n° 14 : Favoriser la détection de faits de corruption à l'étranger en mobilisant l'ensemble des services de l'État.

OUVRAGES RÉCENTS

LES OUTILS DE LA COMPLIANCE

AUTEUR : MARIE-ANNE FRISON-ROCHE

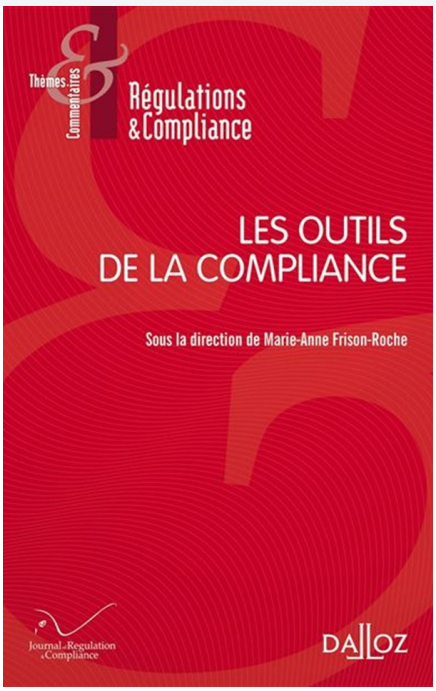
ÉDITEUR : DALLOZ

Résumé

Le Droit de la Compliance se définit par les buts monumentaux qu'il vise.

De gré ou de force, les entreprises doivent se structurer et agir pour les atteindre. Dans une transformation majeure et mondiale, elles deviennent ainsi transparentes, donnant à voir Les *Outils de la Compliance*.

Faire ressortir l'unité de ces outils favorise un régime juridique unifié, tout en les adaptant pays par pays, secteur par secteur, entreprise par entreprise. Comprendre ces Outils de Compliance pour anticiper l'appréciation faite par les régulateurs, superviseurs et juridictions, et les dispositions des prochains textes, tandis que les entreprises sont invitées à en inventer de nouveaux, toujours plus adéquats.



Perspectives générales à travers lesquelles sont scrutés cartographies des risques, programmes de conformité, conventions judiciaires d'intérêt public, formations ad hoc, algorithmes, audits, sanctions, contrôles, lancements d'alerte, actions collectives, etc.

GOUVERNANCE ET ANTICORRUPTION

NATHALIE KALESKI[1]

DIRIGEANTE FONDATRICE DE IKTINOS, SOCIÉTÉ D'ÉTUDES
ET DE CONSEILS EN GOUVERNANCE ET COMPLIANCE,
SECRÉTAIRE GÉNÉRALE DE L'ASSOCIATION FRANCE AUDACIEUSE

La montée en puissance d'un cadre normatif mondial anticorruption, ainsi que la sévérité accrue des autorités de différents pays avec l'augmentation du montant des sanctions, ont incité les entreprises à intégrer la norme anticorruption dans leur stratégie. Mais qu'en est-il de leur gouvernance : quel est l'impact de la lutte anti-corruption sur leur gouvernance, et réciproquement de leur gouvernance sur le risque de corruption ?

Comment les instances dirigeantes[2] prennent-elles en compte le risque de corruption dans l'élaboration de la stratégie de l'entreprise ? Et comment, de leur côté, les conseils d'administration ou de surveillance supervisent-ils la politique de gestion du risque de corruption élaborée par les instances dirigeantes pour s'assurer que la culture éthique est réellement insufflée au coeur de la gouvernance de l'entreprise par des dirigeants exemplaires ?

Selon un rapport de l'OCDE[3], dans la plupart des affaires de corruption, les dirigeants sont impliqués dans les actes incriminés ou en sont au moins informés. Il est donc nécessaire d'impliquer la gouvernance et de renforcer la surveillance au plus haut niveau.

C'est également parce que la prévention de la corruption relève de la gouvernance de l'entreprise à son plus haut niveau que l'Agence française anticorruption (AFA) demande à rencontrer les administrateurs des entreprises qu'elle contrôle. Et, de son côté, l'Institut Français des Administrateurs (IFA) rappelle le rôle déterminant du conseil d'administration dans les différentes phases de maîtrise des risques de fraude et de corruption. La corruption est en effet considérée comme l'échec de la gouvernance, voire pire : une faute organisationnelle[4] ou l'expression d'une politique déviante[5].

I. Implication obligatoire de l'instance dirigeante dans la lutte anticorruption

Avec le dispositif de l'article 17 de la loi 2016-1691 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « Sapin 2 », du 9 décembre 2016, la lutte anticorruption est passée d'une logique curative à une logique préventive : cette loi est une spécificité française qui se distingue des lois anticorruption des autres pays, en ce qu'elle sanctionne l'absence de dispositif de prévention de la corruption, indépendamment de toute réalité de corruption.

C'est ainsi que les dirigeants des sociétés assujetties audit article 17 doivent, sous peine de sanctions administratives et pénales, prendre des mesures destinées à prévenir et à détecter les faits de corruption ou de trafic d'influence[6]. La mise en place de la norme anticorruption

incombe personnellement au dirigeant[7]. En accroissant ainsi les responsabilités des instances dirigeantes, cette norme relève donc de la gouvernance et va de pair avec la professionnalisation du conseil d'administration.

Parce que cet engagement de l'instance dirigeante a de fortes conséquences pour l'entreprise dans sa prévention de la corruption, l'AFA l'examine particulièrement lors de ses contrôles. L'Agence demande également un engagement opérationnel de la part de l'instance dirigeante. Ainsi, à l'occasion de l'actualisation de ses recommandations en janvier 2021, l'AFA a expressément renforcé la responsabilité et le rôle clef de l'instance dirigeante dans la lutte contre la corruption : elle a redéfini ses recommandations aux entreprises autour de trois piliers, l'engagement de l'instance dirigeante étant le premier d'entre eux.

Cette volonté de rechercher la responsabilité personnelle des dirigeants va de pair avec un renforcement des sanctions à leur encontre, même en cas de délégation de pouvoirs[8]. Car, à chaque infraction de corruption, se pose la question de savoir si, et dans quelle mesure, les dirigeants étaient au courant. De manière générale, ils sont poursuivis parallèlement à leur entreprise, au motif qu'ils ne pouvaient ignorer l'existence d'actes de corruption, quand ils ne les ont pas commis eux-mêmes[9]. Les dirigeants se doivent donc d'être proactifs dans la politique anticorruption de leur entreprise : en cas d'affaire de corruption leur niveau d'engagement personnel sera évalué et pèsera sur le dénouement des poursuites pénales.

II. Importance de l'implication des organes de surveillance et de contrôle dans la lutte anticorruption

L'AFA recommande l'implication et l'exemplarité des instances dirigeantes. Mais que faire quand cet engagement est trop « imperceptible »[10], voire quand les dirigeants sont gravement défaillants ? Les organes de contrôle que sont les conseils d'administration et de surveillance doivent intervenir.

Le rôle de l'administrateur ou du membre du conseil de surveillance est alors de décider s'il y a lieu de lancer une enquête. Ce qui est possible et même souhaitable, car il est indépendant de l'entreprise, à la différence du dirigeant. Les praticiens conseillent de mettre en place au minimum un rapport direct du responsable de la compliance avec le conseil, compte tenu du risque pénal. Ce qui peut s'avérer difficile quand le dirigeant veut tout contrôler, y compris l'enquête.

Favorable à cette interaction de la compliance avec les organes de gouvernance, et au renforcement du rôle du conseil d'administration et du conseil de surveillance, l'AFA a toujours voulu s'assurer de l'engagement fort non seulement de l'instance dirigeante, mais aussi des conseils, alors que cet engagement n'est pourtant pas prévu par la loi : lors de ses contrôles, elle rencontre toujours un membre du conseil d'administration.

C'est pourquoi dans son projet d'actualisation de recommandations soumis à consultation publique, l'AFA recommandait « que le dispositif anticorruption et ses actualisations périodiques soient validés par le conseil d'administration ». La version définitive est toutefois en retrait par rapport audit projet, car il n'y est plus question de validation, mais seulement de présentation[11].

Cependant, quels que soient le rattachement et le positionnement de la fonction compliance, son responsable doit pouvoir interagir directement avec tous les organes de la gouvernance, notamment le conseil d'administration ou de surveillance. Car, si les dirigeants exécutifs endossent une responsabilité personnelle dans la mise en oeuvre du programme de conformité, cette mise en oeuvre doit se faire sous la supervision du conseil, gardien des valeurs d'éthique et de compliance de l'entreprise.

Dans deux notes de synthèse de sa commission déontologie[12], l'IFA (Institut Français des Administrateurs) souligne le rôle déterminant du conseil dans les différentes phases de maîtrise des risques de fraude et de corruption. Le conseil « doit, dans son rôle de contrôle et de supervision, s'informer et surveiller le correct déploiement et l'efficacité du dispositif mis en place par la direction générale pour réduire ces risques ». Il s'agit de « recueillir auprès de la direction générale les éléments qui montrent que la démarche entreprise est concrète et réelle,

par opposition à de grands principes non appliqués ». Il doit enfin vérifier l'existence et la pertinence du processus de compliance[13].

L'IFA préconise donc un engagement fort et personnel du conseil, suivant en cela l'approche anglo-saxonne qui réclame l'implication active, non seulement des dirigeants, mais également du conseil. De ce fait, les administrateurs endossent une responsabilité spécifique.

III. Améliorer la gouvernance en renforçant le rôle des organes de surveillance et de contrôle dans la lutte anticorruption

Dans les dernières révisions de son code, l'AFEP-MEDEF a certes souhaité renforcer les missions du conseil d'administration dans ce domaine, mais avec cependant une réserve. L'article 1.6 de ce code dispose à propos du conseil d'administration : « Il s'assure, le cas échéant (souligné par nous), de la mise en place d'un dispositif de prévention et de détection de la corruption et du trafic d'influence. Il reçoit toutes les informations nécessaires à cet effet ».

Cette réserve peut s'expliquer par le fait que toutes les entreprises ne sont pas assujetties à l'article 17 de la loi Sapin 2 et n'ont donc pas l'obligation légale de mettre en place un tel dispositif. Mais, à défaut d'appliquer le dispositif même de l'article 17 avec ses contraintes, l'article 1.6 précité pouvait préconiser l'adoption de tout dispositif assurant la protection de l'entreprise dont les actionnaires sont en définitive représentés par les membres des conseils.

Il s'agit là d'une position en retrait par rapport à celle de l'IFA, qui se retrouve dans la pratique des entreprises. Selon une enquête réalisée conjointement par Labrador, Ethics & Boards et EY (Panorama de la gouvernance, 2019), seuls 33 % des conseils des sociétés du SBF 120 mettent les thématiques de l'éthique et de la compliance à leur agenda. Cela malgré un contexte de contrôles accrus effectués par l'AFA auprès des entreprises françaises, sans compter les menaces de poursuites par des autorités étrangères, et enfin les demandes des grands groupes de voir leurs clients et fournisseurs se conformer aux obligations de lutte anticorruption[14].

Il serait donc souhaitable de retirer les mots « le cas échéant » de l'article 1.6 précité, alors qu'aux termes mêmes de ce code AFEP-MEDEF, les administrateurs « ont le devoir (*souligné par nous*) de demander l'information utile dont ils estiment avoir besoin pour accomplir leur mission » (article 12.3) et « doivent pouvoir rencontrer les principaux dirigeants de la société, y compris hors la présence des dirigeants mandataires sociaux » (article 11.3).

Ce code préconise en outre, dans certains cas, la désignation d'un administrateur référent « en matière de gouvernance ou de relations avec les actionnaires » (article 3.3). Il conviendrait de rendre obligatoire la désignation d'un tel administrateur référent en charge du suivi de la politique anticorruption. Celle-ci, faut-il le redire, concerne au premier chef les actionnaires, vu l'impact d'un acte de corruption sur la valeur de l'entreprise.

Pour être efficacement au coeur de la stratégie de l'entreprise et développer une culture d'intégrité seule capable d'éviter le piège d'une politique de compliance formaliste, l'anticorruption doit donc figurer à l'ordre du jour des travaux des conseils d'administration ou de surveillance.

Mais la supervision des dirigeants par les conseils a aussi ses limites, en raison de possibles conflits d'intérêts entre les actionnaires et les salariés. C'est pourquoi la gouvernance doit s'attacher à prendre en compte les intérêts de l'ensemble des parties prenantes, ce qui impacte la stratégie de l'entreprise comme son modèle économique.

Notes :

1. Auteur de l'étude *Les Entreprises face au défi de l'anticorruption*, Institut Friedland-CCI Paris-Idf, décembre 2018.
2. On entend par *instances dirigeantes* les « personnes placées à la tête de l'organisation et chargées de la gérer, en application de ses statuts et des normes en vigueur » (Recommandations de l'AFA, Journal Officiel du 12 janvier 2021).
3. OCDE 2014: « *Rapport de l'OCDE sur la corruption transnationale : Une analyse de l'infraction de corruption d'agents publics étrangers* », Éditions OCDE. http://dx.doi.org/10.1787/9789264226623-fr ; ce rapport analyse 427 affaires de corrup-

tion transnationale, terminées depuis l'entrée en vigueur, le 15 février 1999, de la *Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales.*

4. Ce sont les termes des juges dans le dossier Total (Arrêt cour d'appel de Paris 26 février 2016 -n°13/09208).

5. Dans le dossier Alcatel, la Cour de cassation (arrêt du 16 juin 2021, 20-83.098 F-P – Chambre criminelle) approuve l'arrêt de la Cour d'appel en ce qu'elle « considère que la multiplication de paiements illicites, dans des zones géographiques différentes, ne saurait être uniquement le résultat de la collusion de deux salariés, mais constitue l'expression d'une politique du groupe, déterminée par la société par la mise en place d'une organisation complexe laquelle, pour les contrats d'agents, sous couvert de transparence et de collégialité, en prévoyant une multitude de documents et une pluralité d'intervenants, n'avait d'autre but que de diluer les responsabilités, chacun des intervenants ayant une responsabilité déterminée, et permettre, sous une apparence de légalité, la poursuite des contrats d'agents permettant des paiements illicites à des décideurs publics étrangers qui étaient déterminants pour les résultats commerciaux de l'entreprise ».

6. L'article 17 de la loi Sapin 2 vise les présidents, les directeurs généraux et les gérants, et selon les attributions qu'ils exercent, les membres du directoire des sociétés anonymes régies par l'article L.225-57 du Code de commerce, dans les entreprises d'une certaine taille (l'effectif comprend au moins cinq cents salariés et le chiffre d'affaires est supérieur à 100 millions d'euros).

7. En cas de manquement à l'obligation de mise en place du dispositif prévu à l'article 17 précité, le dirigeant encourt jusqu'à 200 000 € d'amende, nonobstant toute délégation de pouvoirs.

8. Ainsi, le Tribunal judiciaire de Paris a validé le 26 février 2021 la convention judiciaire d'intérêt public (CJIP) entre le PNF et les sociétés Bolloré S.E. et Financière de l'Odet S.E. mais a refusé d'homologuer la comparution avec reconnaissance préalable de culpabilité (CRPC) pour les dirigeants, décidant que l'affaire nécessitait un procès pénal pour ces derniers.

9. Le rapport précité de l'OCDE indique que dans 12% des 427 affaires de corruption analysées, le PDG était informé de la corruption et l'a approuvée.

10. Dans son rapport annuel d'activité 2020, l'AFA indique: « Bien qu'en progrès, l'engagement des instances dirigeantes reste imperceptible dans un certain nombre de cas, surtout en début de contrôle, et se limite trop souvent à la signature de la préface des codes de conduite » (page 20). L'agence souligne que la qualité du dispositif de prévention prévu par l'article 17 varie selon le niveau d'engagement de l'instance dirigeante (page 21).

11. Recommandations publiées au Journal Officiel du 12 janvier 2021, paragraphe 95, page 14: les membres des conseils d'administration ou autres organes de contrôle ou de surveillance « s'assurent, dans le cadre de leur mission de surveillance des activités de l'entreprise, de l'existence, de la pertinence et de l'efficacité des mesures prises par les dirigeants afin de se conformer à leurs obligations légales. Pour ce faire, dans les sociétés dotées de tels organes, l'AFA recommande que le dispositif anticorruption et ses actualisations leur soient périodiquement présentés afin qu'ils disposent de toutes les informations nécessaires pour veiller à la conformité de l'entreprise à l'article17 de la loi ».

12. « Rôle du conseil d'administration en matière d'éthique » (octobre 2012) et « Rôle du conseil en matière de gestion du risque de fraude et de corruption » (novembre 2014).

13. Les grandes étapes de ce processus sont:

- sensibilisation et prévention : le conseil doit s'assurer de la cohérence et de l'effectivité du dispositif, notamment en termes de ressources et de compétences ; l'exemplarité du management est essentielle, elle concerne également le conseil qui peut être amené à montrer un engagement fort en se formant lui-même,

- détection et investigation : le conseil doit s'assurer de la mise en oeuvre des investigations et s'informer des résultats des plans d'action ; il pourra être amené à suivre les cas les plus critiques, voire, en cas de mise en cause directe ou indirecte de la direction générale, s'investir personnellement dans l'investigation ; c'est pourquoi le responsable de la compliance doit pouvoir accéder au conseil, hors la présence du directeur général ou du président,

- suivi des actions correctives et communication : le conseil doit s'informer de la bonne mise en oeuvre des mesures de remédiation, notamment auprès de l'audit interne, et encourager l'entreprise à communiquer sur son dispositif de compliance.

14. Ces demandes sont formulées dans le cadre de l'évaluation des tiers (fournisseurs ou clients) qui doit être faite selon de dispositif de l'article 17 précité.

Inscription à la revue du GRASCO

Par mail : abonnement@larevuedugrasco.eu

Diffusion gratuite de vos offres d'emploi, événements, manifestations et parutions ouvrages[1]

Par mail : information@grasco.eu

1 après validation de la rédaction

BANQUES SUISSES ET RÈGLES ANTI-BLANCHIMENT

CARLO LOMBARDINI

AVOCAT AU BARREAU DE GENÈVE,
PROFESSEUR À L'UNIVERSITÉ DE LAUSANNE (SUISSE)

Pour les banques, la lutte contre le blanchiment est difficile pour divers motifs.

D'abord, parce que faisant le commerce de l'argent, les banques sont visées de plein fouet par la réglementation adoptée. Elles n'ont pas le choix mais doivent respecter rigoureusement les exigences posées. Les erreurs se payent très cher et pendant longtemps.

Ensuite, parce que certains groupes bancaires sont des colosses. Il est difficile de savoir ce qui se passe réellement au sein de groupes qui ont des dizaines de milliers d'employés implantés aux quatre coins de la planète et qui offrent leurs services à d'innombrables clients venant d'horizons géographiques, politiques et économiques divers.

Enfin, les banques sont là pour servir leurs clients avec diligence, ce qui signifie notamment agir rapidement dans l'ouverture des comptes, l'acceptation de fonds ou l'exécution de transferts. Or, les exigences de la réglementation contre le blanchiment rendent plus chères et plus difficiles ces prestations.

I. Le cadre légal suisse anti-blanchiment

Le cadre suisse de la lutte anti-blanchiment se présente comme suit :

- deux dispositions du Code pénal (CP) : les art. 305bis et 305ter [1] ;
- une loi cadre : la Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme[2] ;
- une ordonnance sur le blanchiment[3] édictée par l'autorité de surveillance des établissements financiers, notamment des banques[4] (FINMA) ;
- un texte issu de l'autoréglementation qui lie les diverses banques suisses : la Convention relative à l'obligation de diligence des banques[5].

La loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA) pose les exigences que les intermédiaires financiers doivent respecter dans la lutte contre le blanchiment d'argent. Au nombre des intermédiaires financiers, on distingue ceux qui sont soumis à réglementation parce qu'ils exercent une activité soumise à autorisation dans le domaine financier (art. 2 al.2 LBA : banques, gestionnaires de fortune, assurances, maisons de titres, acteurs divers dans le domaine des placements collectifs de capitaux...) de ceux qui « à titre professionnel, acceptent, gardent en dépôt ou aident à placer ou à transférer des valeurs patrimoniales appartenant à des tiers » (art 2 al.3 LBA).

L'ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA) contient les exigences organisationnelles qui doivent être respectées par le secteur financier, notamment bancaire en matière de lutte anti-blanchiment.

La Convention relative à l'obligation de diligence des banques (CDB) règle plutôt des exigences de nature formelle qui concernent l'identification du co-contractant et de l'ayant droit économique d'avoirs.

Enfin, l'obligation de communiquer des soupçons fondés de blanchiment est contenue à l'art. 9 LBA ; le droit de communiquer des soupçons à l'art. 305ter al.2 du CP.

Cet amoncellement de textes est le fruit de l'histoire. En théorie, le texte essentiel est la LBA. En pratique : le premier texte a être adopté était la Convention de diligence en 1977 qui a été révisée à plusieurs reprises ; en 1990, l'art. 305bis et 305ter al.1 du CP sont entrés en vigueur ; en 1994, l'art. 305ter al.2 du CP a introduit le droit de communiquer les soupçons de blanchiment d'argent ; la LBA a été adopté à la fin 1997 ; l'OBA-FINMA est régulièrement révisée pour tenir compte de l'évolution des exigences internationales en la matière et au gré de diverses affaires qui ont secoué la place financière.

II. Qu'est-ce que le blanchiment ?

Le terme blanchiment est utilisé régulièrement tant par l'autorité de poursuite pénale que par l'autorité de surveillance.

A. Pour l'autorité de poursuite pénale

Pour l'autorité de poursuite pénale, les normes pertinentes sont les art. 305bis et 305ter du CP. À teneur de l'art. 305bis du CP[6], le blanchiment se définit comme un acte propre à entraver l'identification de l'origine, la découverte ou la confiscation de valeurs patrimoniales provenant d'un crime ou d'un délit fiscal qualifié et ce, avec conscience et volonté.

Une banque peut être responsable pénalement directement aux conditions de l'art. 102 al. 2 du CP[7].

L'art. 305bis du CP doit être lu avec l'art. 305ter al. 1 du CP[8] qui oblige les personnes actives dans le domaine financier (les intermédiaires financiers au sens de la LBA mais nous nous référerons aux banques) à identifier l'ayant droit économique des valeurs qui leur sont confiées.

Il convient de souligner que le droit suisse ne définit pas l'ayant droit économique. La notion d'ayant droit économique est pertinente pour les comptes détenus par des personnes physiques ou des sociétés dites de domiciles. Pour les autres sociétés (sociétés dites opérationnelles), la notion pertinente et celle de détenteur de contrôle, qui concerne non les avoirs en compte mais le titulaire du compte lui-même. Eu égard à la teneur de l'art. 102 al. 1 du CP, seules des personnes physiques seront en principe responsables pour la violation de l'art. 305ter al. 1 du CP.

Le processus d'identification ne doit pas être purement formel (un nom sur un formulaire) ; pour identifier l'ayant droit économique des valeurs, les banques doivent s'interroger sur la relation qui peut exister entre la personne désignée en qualité d'ayant droit économique et les valeurs concernées par la relation d'affaires.

Dans les cas les plus risqués et/ou complexes, l'identification nécessite une réflexion sur la cause juridique liée à l'acquisition des valeurs par la personne désignée comme ayant droit économique. On ne devient pas ayant droit économique de valeurs simplement parce que celles-ci sont créditées sur un compte. On le devient parce qu'une cause juridique légitime ce crédit : *credendi causa, donandi causa ou solvendi causa.* Et la discussion sur la cause juridique permet de passer de la problématique de l'art. 305ter al. 1 du CP à celle de l'art. 305bis du même code.

B. Pour les autorités de surveillance

Alors que l'autorité de poursuite pénale s'intéresse aux infractions susmentionnées qui doivent, en théorie, être à tout le moins au stade de la tentative, les autorités de surveillance sont concernées par le risque de blanchiment d'argent.

Même si aucun acte de blanchiment concret n'est détecté, un établissement peut être sanctionné si des défaillances organisationnelles facilitent d'éventuels actes de blanchiment.

Même si leur approche est différente, Le droit de la surveillance et le droit pénal se rejoignent de façon très dangereuse pour une banque : les constatations, en général négatives, faites par l'autorité de surveillance, avec qui la banque va collaborer sans réserve, sont transmises par celle-ci à l'autorité pénale. Et cette dernière va ensuite les utiliser pour alimenter son dossier et démontrer que la banque n'a pas « pris toutes les mesures d'organisation raisonnables et nécessaires pour empêcher » une infraction (art. 102 al. 2 du CP).

III. Les procédures pénales pour blanchiment

Les procédures pénales pour des actes de blanchiment se multiplient contre des banques et/ou des personnes physiques travaillant pour ces établissements. Elles suscitent l'intervention de l'autorité pénale suisse et, parfois, étrangère, ainsi que de la FINMA,

voire même d'autres autorités de surveillance.

Les procédures pour blanchiment d'argent sont souvent longues ; au sein d'une banque des ressources massives sont mobilisées pour les gérer, comprendre ce qui s'est passé, récolter les documents nécessaires à cet effet et assurer une coopération totale et sincère avec l'autorité de surveillance. De nombreux employés, à tous les niveaux, peuvent être entendus par la justice, voire même interpellés, poursuivis ou renvoyés en jugement. Ce qui conduit à des perturbations notables dans la conduite ordinaire des affaires et entrave sérieusement l'activité professionnelle des personnes ciblées par les autorités.

La survenance de cas de blanchiment au sein d'une banque suscite des risques multiples de nature diverse. Ces derniers vont au-delà du seul risque juridique lié à la condamnation qui pourrait être prononcée au terme d'une procédure pénale. Les risques encourus peuvent être :

- financiers : du fait des montants des amendes et d'autres sanctions pécuniaires encourues par l'établissement ;

- réputationnels : compte tenu des explications qui peuvent devoir être données aux actionnaires, aux employés, aux clients et au public ;

- stratégiques : l'existence d'une procédure pénale visant un établissement doit être annoncée aux diverses autorités de surveillance des pays dans lesquels la banque déploie son activité ;

- existentiels : l'autorité de surveillance peut retirer l'autorisation d'exercer l'activité à un établissement si elle estime qu'il n'est pas à même de gérer de façon appropriée les risques liés au blanchiment d'argent.

IV. Lutte anti-blanchiment et organisation bancaire

Les autorités pénales s'intéressent lors des enquêtes pour blanchiment d'argent au cadre organisationnel et réglementaire des établissements visés par les procédures. Il se justifie donc de fournir des indications générales à ce propos.

A. Le conseil d'administration

En droit suisse, le conseil d'administration d'une banque n'est pas chargé de gérer l'établissement. Les banques suisses ne peuvent pas avoir d'administrateurs dits délégués. Le conseil d'administration fixe la stratégie et pose le cadre général de l'organisation et du fonctionnement de la banque. Il définit l'appétence au risque de la banque (soit l'étendue et la mesure des risques qu'elle veut courir) et s'assure que l'établissement dispose des moyens d'identifier et de gérer ces risques en respectant les limites que le conseil a fixées. Il surveille les mesures prises par la direction au titre du contrôle interne. Le conseil est également chargé de surveiller la direction.

Dans l'exercice de ses fonctions, le conseil d'administration est aidé par l'auditeur dit externe et l'auditeur dit interne. L'auditeur externe est une société tierce qui surveille non seulement le respect des règles comptables (audit dit comptable) mais également les règles prudentielles (audit dit prudentiel). Le système suisse est un système de surveillance dit dualiste où ces sociétés interviennent aux côtés de la FINMA pour la surveillance des banques. Elles deviennent les yeux de l'autorité. La société d'audit rédige des rapports annuels, qui ne sont pas publics, à l'attention de la FINMA et du conseil d'administration de la banque qui l'a mandatée. Toute une partie du rapport d'audit prudentiel est consacré aux règles en matière d'anti-blanchiment édictées par la banque et à leur respect.

L'auditeur interne répond directement au conseil d'administration. Il représente la troisième ligne de défense. Il participe à la sauvegarde des intérêts de la banque avec la première et deuxième ligne de défense. Il intervient ex post en examinant la conformité du comportement de la direction aux mesures prises par le conseil. Le conseil doit coordonner les travaux de l'auditeur externe et de l'auditeur interne en matière de respect des prescriptions anti-blanchiment.

Enfin, le conseil d'administration reçoit du service compliance « *une analyse des risques dans la perspective de la lutte contre le blanchiment d'argent et du financement du terrorisme* » (art. 25 al. 2 OBA-FINMA).

Précisons pour conclure sur le rôle du conseil que souvent ce sont les comités d'audit et/ou de risques au sein du conseil qui suivent plus particulièrement les thèmes évoqués ci-dessus.

B. La direction

C'est la direction qui est principalement compétente en matière de lutte contre le blanchiment d'argent. On distingue au sein de la direction et des employés qui dépendent d'elle, d'une part, la première ligne de défense (le front ou les unités d'affaires génératrices de revenus) et, d'autre part, les

instances de contrôle indépendantes (deuxième ligne de défense), notamment contrôle des risques[9] et fonctions de compliance[10].

i. Le système de contrôle interne

La direction doit s'occuper « *de la conception et de l'entretien de processus internes adaptés, d'un système d'information du management approprié et d'un SCI* (système de contrôle interne) *ainsi que d'une infrastructure technologique adéquate* » (ch. 50 Circulaire FINMA Gouvernance Banques 2017/1, ci-après Circulaire 2017/1)[11].

Le SCI recouvre les règles d'organisation et de fonctionnement de la banque dans l'exercice de son activité pour mettre en oeuvre la stratégie fixée par le conseil d'administration dans le respect des exigences légales et réglementaires d'une part, de l'appétit en matière de risques également défini par le conseil, d'autre part. La réglementation anti-blanchiment d'une banque et son application relèvent du SCI de l'établissement.

Pour que le SCI soit efficace, les divers intervenants doivent être au clair sur leurs fonctions et disposer des moyens adéquats pour les exercer. Des systèmes d'identification et de mesure des risques adaptés aux activités et à l'organisation de l'entreprise doivent exister. Les principales informations issues de ces systèmes doivent être disponibles. Les contrôles effectués et leurs résultats doivent être documentés. D'éventuelles dysfonctions doivent être corrigées et les instances compétentes au sein de l'établissement informées pour déterminer les conséquences, par exemple en matière de ressources humaines, de réglementation, de processus ou de surveillance.

En matière d'anti-blanchiment, les thèmes suivants sont importants :

- l'ouverture des comptes ;
- l'identification correcte des clients, des ayants droit économiques et des détenteurs de contrôle ;
- l'identification de la clientèle à risque accru, notamment les personnes politiquement exposées (PEPs) et les diverses catégories qu'ils représentent ;
- la mise en place d'un système permettant de classifier les risques présentés par les clients et leurs transactions ;
- l'origine des fonds des clients et l'activité économique de ces derniers ;
- l'utilisation des comptes et le volume de transactions intervenues par rapport à ce qui était attendu ;
- l'identification de transactions, d'entrées ou de sorties des fonds, qui nécessitent des clarifications complémentaires ;
- la revue régulière des dossiers clients pour s'assurer de leur mise à jour ;
- la revue régulière des clients, des ayants droit économiques et des détenteurs de contrôle ;
- le paramétrage du système informatique, notamment la fixation des indicateurs de risques[12] ;
- la clôture dans les délais des alertes informatiques ;
- les activités d'investigation, notamment si les transactions sur un compte ne correspondent pas à ce qui est attendu ou s'il apparaît que le client a donné des indications fausses à l'établissement ;
- l'examen de transactions sur des comptes liés entre eux ;
- la communication de soupçons aux autorités.

Le processus anti-blanchiment ne doit pas se dérouler simplement lors de l'ouverture du compte mais se poursuit au gré de ce que la vie de ce dernier et l'évolution de la situation des clients (ainsi que des détenteurs de contrôle ou ayants droit économiques) révèlent.

Les règles du SCI doivent déterminer :

- qui est en charge des diverses tâches de contrôle,
- si une ou plusieurs personnes interviennent pour exercer ces tâches et comment elles se répartissent les rôles,
- quels sont les contrôles qui existent, comment ils sont effectués, par qui ,
- quelle est l'étendue de l'analyse nécessaire (de la plausibilité à la quasi-certitude ; du renseignement fourni par le client à sa corroboration par une source externe) selon le degré de risque du client et des transactions.

Tout ce qui est fait doit être documenté. Non seulement ce qui est constaté mais également l'analyse à laquelle on a procédé avec les conclusions que l'on en tire et les décisions que l'on prend. Bien entendu, les personnes participant au processus doivent être identifiées. L'activité bancaire a toujours été bureaucratique ; dans le domaine de l'anti-blanchiment, la tendance s'est encore accrue eu égard d'ailleurs au texte de l'art. 7 al. 1 LBA qui pose un principe de portée générale[13].

ii. Le rôle de la première ligne de défense

Les activités de contrôle doivent d'abord avoir lieu au niveau de

la première ligne de défense, soit des personnes en contact direct avec la clientèle.

La première ligne de défense joue un rôle important puisqu'elle est censée connaître les clients, leurs activités, l'origine de leur fortune et les transactions qu'ils effectuent. Dans l'exercice de ses fonctions, la première ligne de défense doit être régulièrement formée, notamment par l'intervention de spécialistes externes. Elle doit apprendre à ne pas être simplement l'avocate des clients, avec la tentation de croire, parfois de façon touchante, aux histoires plus ou moins convaincantes qu'ils racontent. N'importe qui peut dire toujours oui à un client ; il faut un certain courage pour savoir quand et comment dire non.

iii. Le rôle de la deuxème ligne de défense

Les fonctions de la deuxième ligne de défense doivent aider la première ligne. La lutte anti-blanchiment ne peut être simplement confiée à la première ligne de défense, en espérant que celle-ci dispose de l'esprit critique et de la force de caractère nécessaire pour refuser les mauvais clients ou avoir le courage de les dénoncer. Les caractéristiques d'un gérant qui est un bon « chasseur » de clients ne sont pas les mêmes que celles d'un bon *compliance* ou *risk manager*.

Les personnes au sein de la deuxième ligne de défense doivent disposer d'une très bonne connaissance de l'activité bancaire et savoir comment l'utiliser en pratique. Elles doivent avoir une vision complète et transversale de l'organisation et du fonctionnement de la banque, qui ne soit pas purement théorique. Elles doivent être plus que de simples contrôleurs. Elles doivent connaître les situations et les pratiques qui peuvent être sources de difficultés dans les rapports d'affaires entretenus, pouvoir s'exprimer de façon critique sur l'organisation de la banque et l'adéquation de ses procédures, avoir les capacités d'anticiper et d'identifier les risques qui pointent à l'horizon. La deuxième ligne de défense ne doit pas être simplement un centre de coûts mais contribuer à une création de valeur saine à moyen terme.

La *compliance* joue évidemment un rôle important, paradoxalement peut-être même trop important. La tendance qui existe dans certains établissements à pratiquement refaire faire par le compliance les tâches de la première ligne de défense nous semble erronée. La première ligne de défense est censée connaître le risque et doit assumer ses responsabilités. Les supérieurs hiérarchiques des gérants en contact avec les clients doivent surveiller leurs équipes. La première ligne ne doit pas être déresponsabilisée, ce qui peut arriver si elle pense que d'autres services vont remédier à ce qu'elle n'a pas fait ou a mal fait.

En matière de lutte anti-blanchiment (comme dans les autres domaines), la fonction risque doit fournir une opinion motivée sur l'identification correcte des risques et leur niveau de maîtrise, notamment eu égard à la politique de risque fixée par le conseil. Elle doit déterminer si et comment les risques identifiés peuvent être mitigés. Les mesures prises à cet effet peuvent être opérationnelles (processus d'approbation ad hoc ou contrôles supplémentaires) ou juridiques (amélioration de la documentation, par exemple). Enfin, la réflexion doit également porter sur les risques que l'établissement ne voudrait en aucun cas courir et les mesures qui peuvent être prises pour ne pas devoir les affronter. La fonction risque doit attirer l'attention sur l'existence de nouveaux risques possibles dont la portée n'est pas encore correctement identifiée.

Il apparaît clairement que les instances de contrôle sont multiples, avec l'inconvénient que le processus devienne bureaucratique, que chaque instance croit que l'autre fait un certain travail et que les questions essentielles soient perdues de vue.

En conclusion, la lutte contre le blanchiment d'argent est un chantier infini. Des règles sont régulièrement adoptées et mises en oeuvre au prix d'efforts et de coûts importants. Mais les autorités, à l'occasion de tel ou tel nouveau scandale, souvent relayé par une certaine presse, estiment que ces règles, qui semblaient indispensables, sont en réalité totalement insuffisantes et l'adoption de nouvelles dispositions encore plus rigoureuses doit être envisagée.

Personne ne se demande si l'approche choisie est correcte ou si le rapport coûts/bénéfices de l'exercice se justifie. Il ne s'agit bien entendu pas d'autoriser ou de faciliter le blanchiment ; mais il n'est pas interdit de porter un regard critique sur ce qui a été fait et va continuer d'ailleurs d'être fait.

D'abord, parce qu'il y a une tendance indiscutable à s'en prendre régulièrement au secteur bancaire. C'est un objectif facile : le secteur est honni par une partie

de l'électorat ; certaines banques ont des comportements peu intelligents et quelques banquiers peuvent être d'une grande arrogance.

Ensuite, parce que les acteurs du secteur privé n'ont pas vocation à conduire des enquêtes et lutter contre la criminalité. C'est en principe la tâche de l'État. On a délégué au secteur bancaire la lutte contre une certaine forme de criminalité. Les banques supportent des coûts très élevés pour un combat difficile. La lutte anti-blanchiment se fait à leurs frais. Les conséquences d'erreurs se paient très cher. Aucune récompense n'est délivrée en cas de travail bien fait.

Enfin, l'étendue des mesures prises a pour conséquence que les banques refusent de fournir des services à certaines catégories de clients pour ne pas encourir de risques. Ce qui est compréhensible dans la perspective des établissements mais est susceptible d'attirer les clients ainsi rejetés vers un système financier parallèle et occulte.

Notes :

1. Code pénal suisse (CP), Recueil systématique du droit fédéral (RS) 311.0.
2. Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA), RS 955.0.
3. Ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), RS 955.033.0.
4. Loi sur l'Autorité fédérale de surveillance des marchés financiers (LFINMA), RS 956.1.
5. https://www.swissbanking.ch/_Resources/Persistent/b/b/5/6/bb567395296e7938825156ac506c7319d6c9651b/ASB_Convention_CDB_2020_FR.pdf
6. *« 1. Celui qui aura commis un acte propre à entraver l'identification de l'origine, la découverte ou la confiscation de valeurs patrimoniales dont il savait ou devait présumer qu'elles provenaient d'un crime ou d'un délit fiscal qualifié, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*

   1bis. Sont considérées comme un délit fiscal qualifié, les infractions mentionnées à l'art. 186 de la loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct et à l'art. 59, al. 1, 1er paragraphe, de la loi fédérale du 14 décembre 1990 sur l'harmonisation des impôts directs des cantons et des communes, lorsque les impôts soustraits par période fiscale se montent à plus de 300 000 francs.

   2. Dans les cas graves, la peine sera une peine privative de liberté de cinq ans au plus ou une peine pécuniaire. En cas de peine privative de liberté, une peine pécuniaire de 500 jours-amende au plus est également prononcée. Le cas est grave, notamment lorsque le délinquant:

   a. agit comme membre d'une organisation criminelle ou terroriste (art. 260er);

   b. agit comme membre d'une bande formée pour se livrer de manière systématique au blanchiment d'argent;

   c. réalise un chiffre d'affaires ou un gain importants en faisant mé-tier de blanchir de l'argent.

   3. Le délinquant est aussi punissable lorsque l'infraction principale a été commise à l'étranger et lorsqu'elle est aussi punissable dans l'État où elle a été commise. »
7. *« 1. Un crime ou un délit qui est commis au sein d'une entreprise dans l'exercice d'activités commerciales conformes à ses buts est imputé à l'entreprise s'il ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise. Dans ce cas, l'entreprise est punie d'une amende de cinq millions de francs au plus.*

   2. En cas d'infraction prévue aux art. 260ter, 260quinquies, 305bis, 322ter, 322quinquies, 322septies, al. 1, ou 322octies, l'entreprise est punie indépendamment de la punissabilité des personnes physiques s'il doit lui être reproché de ne pas avoir pris toutes les mesures d'organisation raisonnables et nécessaires pour empêcher une telle infraction.

   3. Le juge fixe l'amende en particulier d'après la gravité de l'infrac-tion, du manque d'organisation et du dommage causé, et d'après la capacité économique de l'entreprise.

   4. Sont des entreprises au sens du présent titre:

   a. les personnes morales de droit privé;

   b. les personnes morales de droit public, à l'exception des corpora-tions territoriales;

   c. les sociétés;

   d. les entreprises en raison individuelle. »
8. *« 1 .Celui qui, dans l'exercice de sa profession, aura accepté, gardé en dépôt ou aidé à placer ou à transférer des valeurs patrimoniales appar-tenant à un tiers et qui aura omis de vérifier l'identité de l'ayant droit économique avec la vigilance que requièrent les circonstances, sera puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire.*

   2. Les personnes visées à l'al. 1 ont le droit de communiquer au Bureau de communication en matière de blanchiment d'argent de l'Office fédéral de la police les indices fondant le soupçon que des valeurs patrimoniales proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305bis, ch. 1bis. »
9. La *fonction* risque (ch. 69 ss Circulaire gouvernance banques de la FINMA 2017/1 ; dans une circulaire la FINMA expose sa compréhension de la loi) : assure le caractère systématique de la surveillance et de l'établissement de rapports sur des positions-risque individuelles ou agrégées. En tant que composante des analyses quantitatives et qualitatives, cela implique la réalisation de tests de résistance et d'analyses de scénarios dans des conditions commerciales défavorables ; surveille le profil de risque de l'établissement, notamment à l'aune de la tolérance au risque et des limites posées en matière de risques définies par la politique de risque et les principes de gestion des risques à l'échelle de l'établissement ; est impliquée de manière appropriée dans le développement de nouveaux types de produits, services, domaines d'activité ou secteurs de marché ou dans leur extension ainsi que dans les transactions importantes ou complexes ; remet un rapport sur l'évolution du profil de risque de l'établissement et son activité à la direction, au moins une fois par semestre, et au conseil d'administration au moins une fois par an. Par ailleurs *« En cas d'évolution particulière de la situation,* le contrôle des risques en informe la direction et la révision interne en temps utile et, en cas de faits de grande portée, l'organe responsable de la haute direction » (ch. 76 Circulaire 2017/1).
10. Le service de *compliance* (ch. 77 ss Circulaire 2017/1) a les fonctions suivantes : l'évaluation annuelle du risque de *compliance* lié à l'activité de l'établissement et l'élaboration d'un plan d'action axé sur le risque, plan qui doit être approuvé par la direction. Le plan d'action doit aussi être mis à disposition de la révision interne ; la remise à la direction, en temps utile, de rapports sur les modifications importantes de l'évaluation du risque de *compliance* ; la remise à l'organe responsable de la haute direction d'un rapport annuel sur l'évaluation du risque de *compliance* et l'activité de la fonction de *compliance*.
11. Dans les circulaires, la FINMA expose sa compréhension de la loi. Les textes et les principes quelles continnent ne sont pas contraignants, l'administré peut toujours sucité une décision et un contentieux.
12. Autorité de contrôle prudentiel et de résolution (ACPR), 24 décembre 2020, Attijariwafa Bank Europe (amende de 500.000 euros) : *« 23. Selon le grief 4, fondé sur ces dispositions, la société AWBE n'a pas mis en place, dans ses outils de surveillance, de critères ou de scénarios adaptés et spécifiques à son activité de correspondance bancaire, permettant de détecter des opérations suspectes au regard du profil de risque des établissements clients, alors même que les relations de correspondance bancaire transfrontalières sont considérées comme présentant des risques élevés de BC-FT »* https://acpr.banque-france.fr/sites/default/files/media/2021/01/08/210108_decision_awbe.pdf.
13. Art. 7 Obligation d'établir et de conserver des documents

    « 1. L'intermédiaire financier doit établir des documents relatifs aux transactions effectuées ainsi qu'aux clarifications requises en vertu de la présente loi de manière à ce que des tiers experts en la matière puissent se faire une idée objective sur les transactions et les relations d'affaires ainsi que sur le respect des dispositions de la présente loi. »

LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN AMÉRIQUE LATINE : LES DÉFIS DE LA COOPÉRATION

XAVIER COUSQUER

CODIRECTEUR DU PROGRAMME EL PAcCTO DE L'UNION EUROPÉENNE

L'Amérique latine est, depuis de nombreuses années, la région la plus violente du monde[1], cumulant des taux d'homicides dépassant la barre des 100 pour 100 000 habitants, comptant 39 des 50 villes les plus dangereuses du monde[2] et connaissant des taux d'incarcération parmi les plus élevés de la planète. Le crime organisé y est extrêmement répandu et se trouve présent dans la quasi-totalité des pays de la région, sous différentes formes : des cartels mexicains ou colombiens aux *maras* centraméricaines, des groupes criminels nés dans les prisons du Brésil comme le *Primeiro Comando da Capital* ou le *Comando Vermelho,* à de petites structures plus spécialisées dans certains types de délinquance. Si l'essentiel de la criminalité concerne des phénomènes « classiques » de grands trafics – la cocaïne en premier lieu, mais aussi la traite des êtres humains et le trafic de migrants – les activités criminelles ne cessent d'évoluer, de se diversifier et de se spécialiser. Preuve de cette réalité est la croissance préoccupante des délits environnementaux (trafic d'espèces protégées, de bois, orpaillage clandestin) à tel point que certains pays (Colombie et Pérou, par exemple) considèrent que ces trafics représentent aujourd'hui des bénéfices supérieurs pour les groupes organisés à ceux du trafic de stupéfiants. En matière de trafic de drogue, l'on note une diversification vers le trafic de cannabis mais aussi des drogues de synthèse – méthamphétamine et fentanyl en particulier – notamment au Mexique. Le trafic d'armes à feu est également en hausse dans l'ensemble de la région et, bien évidemment, les délits connexes à ces nombreuses activités criminelles : blanchiment d'actifs et corruption.

Cette réalité, extrêmement inquiétante, est à l'origine de la mise en place du Programme EL PAcCTO de l'Union européenne (UE) dont l'objectif principal est de soutenir les pays d'Amérique latine (du Mexique à la Terre de feu) afin qu'ils luttent plus efficacement contre ces phénomènes criminels. Premier programme régional de l'UE à englober toute la chaîne pénale (coopération policière, judiciaire et systèmes pénitentiaires), EL PAcCTO aborde également différentes thématiques transversales, notamment le blanchiment, la corruption et le sujet principal de cet article : la cybercriminalité.

Dans le contexte latino-américain, compte tenu des niveaux de criminalité et de la diversité des activités criminelles, l'usage des nouvelles technologies pour la commission de délits ou de crimes – ou pour faciliter celle-ci – est une pratique de plus en plus courante. Par ailleurs, en considérant le volume d'activités criminelles dans la région et sachant que les nouvelles technologies sont désormais impliquées dans la commission d'un nombre croissant de délits[3], l'on peut assez facilement en déduire que la cybercriminalité est fortement répandue sur le continent. En revanche, il semble qu'aucun groupe criminel latino-américain n'ait aujourd'hui développé de compétences très avancées en matière de cybercrime comme cela peut être le cas dans d'autres régions du

monde. Cela n'exclut évidemment pas qu'il puisse y avoir des connexions entre de grands groupes criminels latino-américains et des groupes cybercriminels d'Europe de l'Est ou d'Asie, dans une logique de *crime as a service*[4], même si celles-ci n'ont pu être formellement démontrées à ce stade. De ce fait, la menace cybercriminelle en provenance d'Amérique latine n'est pas aujourd'hui considérée comme prioritaire ni hautement inquiétante. Cela ne signifie évidemment pas qu'il ne faut pas s'en préoccuper.

En effet, en Amérique latine l'usage très important et régulier des réseaux sociaux[5] est répandu. Cette réalité implique une plus grande vulnérabilité, notamment en matière d'escroquerie en ligne, de *phishing* ou par le biais de *ransomwares*. Par ailleurs, cette situation facilite l'usage des réseaux sociaux par les groupes criminels pour opérer leurs différents trafics : drogues, traite des êtres humains, notamment à des fins de prostitution, vente d'armes ou toute autre activité criminelle qui passe plus facilement sous les radars, compte tenu du volume immense d'échanges quotidiens sur ces plateformes. La pandémie de la COVID-19 a, comme dans d'autres régions du monde, largement accéléré ce phénomène. Les groupes criminels organisés ont démontré à cette occasion, comme c'est malheureusement souvent le cas, une très grande capacité d'adaptation et de résilience face à l'évolution de leur environnement. Il est, par ailleurs, particulièrement notable qu'en Amérique latine, l'augmentation conséquente de l'usage des nouvelles technologies pour la commission de délits ou de crimes, à l'occasion de la pandémie et des diverses restrictions qu'elle a entraînée, s'est appuyée sur les connaissances existantes des délinquants et criminels, c'est-à-dire l'usage des réseaux sociaux classiques et d'Internet. Ceci est très probablement lié à la réalité mentionnée plus haut : l'absence de groupes très spécialisés en matière de cybercrime dans la région, qui utilisent bien plus volontiers le *deep web*, le *dark web* ou des applications ultra sécurisées pour la réalisation ou la gestion de leurs activités criminelles.

Aussi, même si la problématique cybercriminelle en Amérique latine n'atteint pas les niveaux que l'on peut connaître dans d'autres pays et régions de la planète, elle n'en fait pas moins l'objet d'une préoccupation et d'une attention croissantes de la part des institutions publiques de ces pays. Entre 2020 et 2021, le Programme EL PAcCTO a appuyé la réalisation d'une première évaluation de la menace criminelle en Amérique latine, inspirée de l'expérience du SOCTA[6] (Serious and Organized Crime Threat Assessment) européen. L'Instrument de Documentation et d'Évaluation de la menace en Amérique Latine (IDEAL)[7], présenté à Lisbonne le 13 juillet 2021, fait ressortir le cybercrime comme la troisième des sept problématiques considérées comme les plus prioritaires par les sept pays ayant participé à l'exercice. Bien que les informations partagées par les pays participants soient encore limitées, les éléments mentionnés plus haut – usage des réseaux sociaux à des fins délictuelles ou criminelles, notamment – ont été clairement identifiés dans le cadre de cette première analyse de la menace.

Lorsqu'un « terrain de jeu » ne présente pas de réelles limites, mais que les arbitres sont contraints par un espace défini, que les règles n'existent pas ou sont sommairement établies, la présence sur le pré virtuel d'acteurs dont les intentions ne sont ni bonnes ni pacifiques, est un problème grave qui peut potentiellement rapidement dégénérer. Les réponses existent, bien évidemment, et ont été progressivement mises en place mais pas de façon harmonisée dans les pays concernés. Parmi ces réponses, le développement de la coopération internationale, qu'elle soit policière ou judiciaire, fait partie de celles qui ont potentiellement le plus fort impact pour lutter efficacement contre ces phénomènes criminels, tout comme la spécialisation des acteurs chargés de cette lutte. En Amérique latine, ces deux aspects sont aujourd'hui imparfaits voire déficients et obèrent en grande partie la possibilité de lutter effectivement contre la cybercriminalité. Ce constat n'est évidemment pas définitif et des solutions existent pour tenter de remédier à cette situation.

I. La coopération internationale en Amérique latine : un défi

En Amérique latine, la coopération internationale, tant policière que judiciaire, est une notion bien connue et intégrée par les différents acteurs de la chaîne pénale. Pour autant, elle n'en souffre pas moins d'un manque de systématisation et de nombreux problèmes, notamment de coordination, qui diffèrent en fonction de l'institution concernée.

A. Le manque de culture de coopération policière

La coopération policière en Amérique latine n'est pas un concept nouveau mais elle a conservé un caractère souvent « artisanal ». La majorité des échanges s'opèrent

de façon informelle et revêtent plus souvent un caractère personnel qu'institutionnel. La culture du travail en réseau est souvent balbutiante et les changements de mentalité sont longs à intervenir. Par ailleurs, la très importante rotation de personnel qui affecte les unités des forces de sécurité de la grande majorité des pays de la région, ne permet pas de développer des capacités pérennes de travail avec de réels spécialistes de la coopération internationale. Quant aux structures de coopération policière régionale, en particulier AMERIPOL, elles demeurent pour l'heure largement inopérantes faute de moyens et de volonté politique. Malgré des velléités de créer un centre spécialisé en matière de cybercriminalité, AMERIPOL qui demeure une association de forces de police sans personnalité juridique, l'on est encore très loin de pouvoir envisager un équivalent de l'EC3 d'EUROPOL (*Europol CyberCrime Centre*) en Amérique latine. Ce contexte explique, en grande partie, pourquoi la coopération policière en matière de cybercrime en Amérique latine et entre l'Europe et l'Amérique latine est complexe, lente et souvent peu effective.

B. Les obstacles à la coopération judiciaire

Dans le domaine judiciaire, il ne fait pas de doute que la culture de la coopération est plus intégrée que dans le domaine policier, la stabilité des personnels plus grande et, de ce fait, le professionnalisme des acteurs souvent supérieur. L'ensemble des ministères publics d'Amérique latine disposent d'une unité spécialisée en matière de coopération judiciaire internationale, regroupées au sein d'un réseau, sous l'égide de l'Association Ibéro-Américaine des Ministères Publics (AIAMP). Ce réseau est particulièrement actif et permet de nombreux échanges, tant sur des opérations en cours que sur des problématiques communes, bonnes pratiques et expériences partagées. Compte tenu de ces éléments, l'on pourrait aisément considérer que la coopération judiciaire en Amérique latine est professionnelle et efficace et permet donc d'envisager des échanges rapides et fructueux entre pays et institutions de la région et avec d'autres régions du monde. Hélas, le problème n'est, en l'occurrence, pas tant institutionnel ou personnel que normatif et procédural. En effet, la coopération judiciaire en Amérique latine demeure régie par le système des autorités centrales (certains pays de la région en comptent plusieurs, en fonction des instruments internationaux considérés), qui implique que l'essentiel du processus de coopération judiciaire doit transiter par ces autorités. Dans de rares cas (le Chili, par exemple), le ministère public est l'autorité centrale, mais dans la plupart des pays ce rôle est assuré par une institution du pouvoir exécutif (le ministère des Affaires étrangères dans la majorité des cas), ce qui a pour effet de créer un risque de politisation de certains dossiers sensibles – et les possibles blocages afférents – et, dans tous les cas, de ralentir grandement les processus de coopération judiciaire. Dans le cas du cybercrime, où la coopération judiciaire doit faire preuve d'une extrême célérité compte tenu de la très grande volatilité des preuves et de la difficulté à identifier les délinquants ou criminels qui se consacrent à ces activités, il va sans dire que des processus de coopération judiciaire correspondant aux standards du XXème siècle sont très largement dépassés, inopérants et obèrent en grande partie l'efficacité – voire la pertinence – de toute procédure de coopération internationale, ce qui est le cas dans la quasi-totalité de ces affaires.

C. Spécialisation et coordination

La complexité technique des affaires de cybercrime implique un haut degré de spécialisation des acteurs de la chaîne pénale, qui existe rarement dans les pays d'Amérique latine tant au niveau des forces de sécurité qu'au sein du Parquet (qui joue, dans la quasi-totalité de ces pays, un rôle majeur dans les enquêtes criminelles). Cela s'explique essentiellement par deux raisons. En premier lieu, car la cybercriminalité est une problématique nouvelle et qui ne représente pas encore une menace de premier ordre dans des pays qui ont, depuis longtemps, concentré leurs efforts de spécialisation en matière de narcotrafic. En second lieu, dans la plupart des pays, les moyens sont limités que ce soit en termes de formation mais surtout de ressources pour recruter plus de personnels. Si l'on y ajoute la très forte rotation du personnel, déjà mentionnée plus haut, l'on peut en outre en déduire que ces faibles ressources ne sont pas utilisées de façon optimale. La conséquence de cette situation est que, si la grande majorité des pays d'Amérique latine ont mis en place des unités spécialisées en matière de cybercrime au sein des forces de sécurité et des ministères publics, celles-ci sont de taille réduite (6 personnes pour l'unité de la police uruguayenne en 2019) et leur niveau de spécialisation est, sauf exception, relativement faible. Sans parler, bien

évidemment, des pouvoirs judiciaires au sein desquels la spécialisation est quasiment inexistante, ce qui n'est pas sans poser de problème pour le jugement de ce type d'affaires et le prononcé de condamnations, lorsque des juges, qui n'ont aucune connaissance de la problématique et souvent des difficultés à la comprendre, sont appelés à trancher.

À cette situation difficile, s'ajoutent d'importants problèmes de coordination, interinstitutionnels mais aussi souvent intrainstitutionnels. Ce qui doit être un réflexe naturel ne l'est souvent pas en Amérique latine où les unités spécialisées fonctionnent de manière cloisonnée. La plupart des institutions ont fait le choix de ne pas doter les unités spécialisées en matière de cybercrime de compétences formelles de coopération internationale, préférant centraliser les procédures au sein des unités de coopération internationale ou des Bureaux Centraux Nationaux Interpol dans le cas des forces de sécurité. L'absence de dialogue et de coordination entre ces différents acteurs s'avère souvent néfaste pour le bon fonctionnement de la coopération internationale. Il n'est malheureusement pas rare de voir, en Amérique latine, une information arriver au Bureau Central National Interpol et n'être transmise au service compétent que plusieurs jours ou semaines après sa réception, ou tout simplement jamais… S'ajoute à cela un manque de confiance – parfois de considération – entre enquêteurs et procureurs qui est, évidemment, particulièrement préjudiciable à l'efficacité des enquêtes – impliquant parfois la duplication de procédures – et à tout processus effectif de coopération internationale.

D. L'absence d'harmonisation du cadre normatif

L'efficacité de la coopération internationale repose en grande partie sur l'harmonisation des législations en matière d'infractions et de sanctions entre pays souhaitant coopérer dans un domaine considéré. La très rapide évolution des phénomènes criminels liés à la cybercriminalité et l'extrême adaptabilité des cybercriminels aux cadres normatifs existants est ainsi un défi pour l'ensemble des pays de la planète. Si l'Union européenne, par le biais de l'acquis communautaire et de la mise en place d'un espace commun de justice et de sécurité, fait figure de modèle en matière d'harmonisation des législations, ce qui facilite grandement la coopération internationale, tel n'est pas le cas de l'Amérique latine où les disparités sont importantes.

À l'heure actuelle, 8 pays d'Amérique latine[8] ont ratifié la Convention sur la cybercriminalité du Conseil de l'Europe – dite Convention de Budapest – de 2001, et l'on peut raisonnablement penser que leurs législations nationales sont relativement alignées, à fortiori si l'on considère que les processus de ratification sont récents. Par ailleurs, le Conseil de l'Europe considère que la législation de 4 autres pays[9] de la région est en grande partie conforme aux dispositions de la Convention de Budapest. Entre ces 12 pays, une certaine harmonisation législative existe donc, qui peut permettre de faciliter la coopération internationale en matière de lutte contre la cybercriminalité, mais évidemment aussi avec les 56 autres États parties à la Convention, dont les États membres de l'Union européenne. Pour autant, 6 pays d'Amérique latine ne sont pas parties à la Convention et leurs législations ne semblent pas être en adéquation avec celle-ci, ce qui ne va pas sans poser de potentielles difficultés en matière de coopération dans un contexte de grande proximité géographique et culturelle entre pays de la région. Parmi ces pays, l'on compte le Mexique, particulièrement affecté par le crime organisé, où il a été détecté que les grands cartels faisaient appel à des spécialistes du cybercrime dans une logique de « *crime as a service* ». Ces disparités législatives constituent, à l'évidence, un frein à l'efficacité de la coopération entre pays de la région.

Par ailleurs, si le chapitre III de la Convention de Budapest[10], consacré à la coopération internationale, prévoit un nombre important de mécanismes, en particulier en matière d'extradition, d'entraide pénale internationale (accès aux données et interception notamment), de communication spontanée d'informations, de coopération transfrontalière et un système de points de contact 24/7, il faut souligner qu'elle ne prévoit pas la mise en oeuvre de certaines modalités novatrices de coopération internationale, telles les équipes communes d'enquête, ou l'utilisation de techniques spéciales d'enquête, comme l'infiltration de cyber agents. Face à une criminalité nouvelle, astucieuse et inventive, les États parties ne sont pas incités à mettre en oeuvre ces nouvelles modalités, souvent très efficaces, de coopération internationale, en particulier dans les pays d'Amérique latine qui les découvrent petit à petit et pourraient utilement améliorer leurs pratiques en la matière, par un usage plus systématique sur un spectre criminel plus ample.

Ces différents éléments peuvent laisser à penser – à raison – que la

coopération policière et judiciaire en matière de cybercrime entre et avec les pays d'Amérique latine est un chemin semé d'embuches. Il existe, malgré tout, une forte volonté dans ces pays de progresser sur ces sujets et, compte tenu des importantes marges de progression, des solutions existent afin d'améliorer la situation et de faire en sorte que la coopération internationale devienne plus systématique, fluide et efficace.

II. Quelles solutions face à la situation actuelle ?

L'ampleur du chantier pour faire en sorte que la lutte contre la cybercriminalité, en particulier dans ses aspects de coopération internationale, soit plus efficace est conséquente. Cependant, un certain nombre de solutions existent. Elles reposent en grande partie sur la volonté politique des institutions concernées, qui n'est pas toujours présente, sur la bonne volonté des acteurs concernés et sur la nécessité de construire progressivement des capacités qui ne pourront être acquises du jour au lendemain. Il s'agit donc d'un processus de longue haleine auquel s'attelle le Programme EL PAcCTO, depuis ses débuts en 2017.

A. Construire une culture de la coopération internationale

Lorsque EL PAcCTO a commencé à travailler dans la région, les seuls « réseaux » existants étaient des groupes *WhatsApp*, dont le fonctionnement semblait malgré tout convenir aux acteurs latinoaméricains concernés. La première étape a donc consisté à expliquer ce qu'était un réseau de coopération internationale, qu'il impliquait un minimum de formalisme et des règles de fonctionnement. Sur cette base le programme a impulsé la création de plusieurs réseaux de coopération policière, dont les membres sont officiellement désignés par les responsables des institutions concernées, et a travaillé avec l'AIAMP à la mise en place d'un règlement encadrant le fonctionnement des réseaux de coopération judiciaire existants. La création du réseau de coopération policière baptisé CibEL@ (*Cibercrimen Europa Latino@merica*), en 2019, a permis de poser les bases d'une nouvelle manière de travailler pour les forces de sécurité spécialisées de la région. Ce réseau a pour objectif d'échanger des informations (sans caractère personnel) entre acteurs spécialisés sur des problématiques communes, de nouveau *modus operandi* identifiés, des informations d'intérêt commun mais aussi de faciliter le traitement d'opérations concrètes impliquant plusieurs pays membres du réseau. Il s'agit de créer, petit à petit, une culture de la coopération internationale, largement inexistante à ce stade. Dès 2017, le Programme avait contribué à créer le réseau ELIPSIA (*Europa Latinoamérica Iniciativa de Protección y Seguridad de la Infancia y Adolescencia*) visant à lutter contre les abus sexuels contre les mineurs sur Internet. Une première opération concrète, lancée début 2018, a conduit à l'arrestation de plusieurs pédophiles présumés en Europe et en Amérique latine mais a également permis d'identifier les importantes carences, techniques, technologiques et institutionnelles, dans différents pays latino-américains. Cela a, malgré tout, permis de démontrer qu'il existait une volonté de travailler, mais aussi une nécessité d'avancer progressivement afin de renforcer les capacités. Cette construction progressive se poursuit, depuis lors, avec l'organisation de réunions et d'activités régulières des réseaux concernés afin d'inculquer, petit à petit, des pratiques et des principes essentiels au bon fonctionnement de la coopération internationale. Pour autant, s'agissant d'un changement de mode de fonctionnement, voire de mentalité, dans le travail, il ne fait pas de doute que cette évolution prendra du temps et que l'acquisition de la culture de la coopération internationale sera l'aboutissement de nombreux efforts et d'un processus lent. Cela n'est pas idéal dans un contexte où les responsables, seuls capables d'insuffler ces évolutions, souhaitent obtenir des résultats rapides. Le travail de pédagogie doit donc se poursuivre pour convaincre qu'un chemin a été ouvert et qu'il doit être parcouru afin que des résultats de plus en plus concrets soient obtenus.

B. Renforcer la coordination interinstitutionnelle

Fort du constat que le fonctionnement en silo est quasiment institutionnalisé dans les structures de la chaîne pénale en Amérique latine, et qu'une défiance, souvent réciproque et régulièrement liée à des accusations de corruption, existe entre enquêteurs, procureurs et juges, la possibilité de développer des protocoles de travail simples entre institutions, ou l'organisation de réunions ponctuelles ne semble pas être de nature à pouvoir apporter une réponse réellement efficace aux problèmes qui se posent. Dans ce domaine également, mais plus encore qu'en matière de coopération internationale, l'évolution des mentalités et la génération d'une plus grande confiance entre acteurs implique un changement drastique. C'est la raison pour laquelle le Programme EL PAcCTO a proposé aux pays partenaires la

mise en place d'équipes multidisciplinaires spécialisées. Regroupant enquêteurs, procureurs et personnels spécialisés, en fonction de la thématique abordée par l'équipe, l'objectif est de faire en sorte que ces différents acteurs travaillent effectivement ensemble, en bonne intelligence et dans la poursuite d'un même but. Les premières équipes mises en place (pour l'heure, aucune dans le domaine de la cybercriminalité) tendent à montrer que le changement est lent à s'opérer et ne représente, en aucun cas, une évidence. En revanche, elles mettent en relief la volonté de mieux travailler ensemble et le fait que les problèmes liés aux défiances existantes peuvent rapidement être surmontés. Ces équipes seront appelées à traiter les cas les plus complexes et ceux qui présentent un caractère international, ce qui est presque la règle en matière de criminalité organisée. L'on peut ainsi espérer, au-delà d'un travail initial de renforcement des capacités, que les membres de ces équipes développent progressivement un haut degré de spécialisation, tant dans leur domaine d'intervention qu'en matière de coopération internationale, et que ces acteurs puissent facilement participer à des équipes communes d'enquête, lorsque la situation se présentera. Il s'agit donc d'un modèle qui pourrait être utilement étendu, pour peu qu'il permette aussi de limiter la rotation des personnels et de développer ainsi les compétences sur le moyen terme. Il est, à ce stade, trop tôt pour effectuer un premier bilan du fonctionnement de ces équipes, mais il fait peu de doute que, si les premiers résultats étaient positifs, il serait particulièrement opportun d'inciter les pays et institutions de la région à étendre ce modèle aux différents domaines dans lesquels la criminalité revêt un haut degré de complexité et à mettre en oeuvre des procédures rapides et effectives de coopération internationale.

C. Développer une vision stratégique

En premier lieu, il est souvent difficile en Amérique latine, pour les enquêteurs et les procureurs, de voir au-delà du cas concret qu'ils ont à traiter et de replacer une affaire dans le contexte plus général de la lutte contre la cybercriminalité ou la criminalité organisée en général. Les limites de la coopération internationale, exposées plus haut, n'incitent pas non plus toujours à aller rechercher d'autres éléments, au-delà de ceux qui sont facilement accessibles. Il en résulte une importante difficulté à tirer tous les fils de l'enquête, à identifier les différentes parties prenantes et à remonter les différentes ramifications des réseaux criminels pour parvenir à les démanteler. Dans la plupart des cas, les enquêtes et les poursuites se limitent aux seuls exécutants. Cette question ne peut se réduire à l'absence de vision stratégique. Elle s'explique aussi en grande partie par l'absence de moyens, de spécialisation, parfois de volonté politique, mais aussi – comme c'est le cas dans de nombreux pays du monde – par la volonté d'obtenir des résultats rapides et visibles alors qu'une enquête de longue haleine mobilise des ressources importantes, pendant un temps long, sans que les résultats ne soient visibles à court terme. Il est pourtant essentiel de pouvoir développer, petit à petit, cette capacité à prendre en compte les dossiers dans toute leur complexité et de faire en sorte que les enquêteurs et les procureurs ne s'arrêtent pas aux éléments les plus évidents de l'affaire. La pédagogie, les processus de spécialisation et la capacité à voir le « panorama » complet – mais aussi la complexité – d'une réalité criminelle sont autant d'éléments à mettre en oeuvre afin de faire évoluer les mentalités et les pratiques. Cela ne pourra se faire du jour au lendemain mais, avec un accompagnement adapté sur des enquêtes complexes, il est possible d'améliorer la situation, afin que ces sujets soient abordés dans leur globalité et que la réponse pénale soit adaptée à la réalité de ces phénomènes. Par ailleurs, il ne fait aucun doute que le développement d'une coopération policière et judiciaire active et plus efficace va dans le sens d'une plus grande capacité à aborder les affaires d'une manière plus stratégique et plus complète.

Le développement d'une vision stratégique est également nécessaire afin d'anticiper l'évolution de la réalité cybercriminelle – dont l'évolution et l'adaptation sont extrêmement rapides – mais aussi afin d'apporter une réponse coordonnée à ce phénomène essentiellement transnational. Pour ce qui est de l'anticipation, sur la base de l'IDEAL, déjà mentionné, il sera utile, dans un futur proche, que les pays d'Amérique latine puissent réfléchir au développement d'un outil d'analyse de la menace cybercriminelle sur le modèle du IOCTA[11] (Internet Organized Crime Threat Assessment) de l'Union européenne. Cet outil, outre une analyse de la spécificité de la menace liée au cybercrime, devra permettre d'identifier les possibles évolutions de cette criminalité et, ainsi, d'anticiper le mieux possible la préparation et

l'adaptation de la réponse pénale. Sur un plan plus stratégique, la capacité d'articuler les politiques publiques de lutte contre la criminalité – la cybercriminalité en particulier – entre pays d'une même région et de définir des stratégies communes est une absolue nécessité, dans un contexte où l'approche purement nationale de ces phénomènes ne fait plus sens et se trouve vouée au mieux à l'inefficacité et, au pire, à l'échec. Le lancement d'une initiative pour la création d'un Comité Latino-Américain de Sécurité Intérieure (CLASI), soutenue par le Programme EL PAcCTO, sur le modèle du COSI[12] (Comité permanent de coopération opérationnelle en matière de sécurité intérieure) de l'Union européenne, va dans ce sens. Sa création devrait intervenir au début de l'année prochaine, sous la présidence française du Conseil de l'Union européenne. Composé des ministres de l'Intérieur et de leurs représentants des pays volontaires, cette structure sera informelle dans un premier temps. Sur la base de la première analyse de la menace qui vient d'être réalisée, les ministres devraient être en mesure de définir de premières priorités, des stratégies conjointes et un plan de travail qui pourrait, à terme, s'apparenter au cycle politique de sécurité qui existe au sein de l'Union européenne. En ce sens, il s'agit également de renforcer la coopération entre pays, à un niveau stratégique et non plus seulement opérationnel, afin d'apporter des réponses plus coordonnées aux problématiques criminelles et d'assurer que la volonté politique accompagne effectivement les opérations des acteurs de la chaîne pénale. Il va sans dire que le CLASI pourrait également devenir un interlocuteur privilégié du dialogue en matière de Sécurité entre l'Union européenne et l'Amérique latine, seule autre région du monde, à l'heure actuelle, qui soit en mesure d'adapter les expériences développées au sein de l'Union.

Malgré la coopération souvent encore balbutiante et les nombreuses limites et difficultés mentionnées dans cet article, il existe des raisons d'espérer. Les chantiers à poursuivre ou à mettre en oeuvre sont importants et ambitieux. Dans un certain nombre de cas, ils impliquent un renforcement des ressources – humaines, matérielles et financières – que certains pays d'Amérique latine auront certainement du mal à mobiliser, dans un contexte de crise économique postpandémie. Pour autant, un certain nombre d'autres évolutions nécessaires sont essentiellement organisationnelles ou impliquent un changement de mentalité, mais ne nécessitent pas la mobilisation de ressources supplémentaires. Dans ce cas, la volonté politique, la pédagogie mais aussi le soutien que les pays européens peuvent apporter à leurs partenaires d'Amérique latine est essentiel. L'Union européenne et ses différents mécanismes que nous connaissons aujourd'hui et qui ont fait leurs preuves, ne se sont pas faits en un jour. Il faut accepter que, dans le cas de l'Amérique latine – qui ne dispose évidemment pas du même cadre politique et normatif – les choses prennent du temps. Ce peut être parfois frustrant mais notre soutien, dans un contexte ou des dynamiques positives s'engagent, est nécessaire afin de créer une relation de confiance et de rechercher des modalités de coopération plus efficaces, avec une région qui partage nos valeurs, nos ambitions et une grande partie de nos préoccupations. Vive la coopération !

Notes :

1. Selon une étude de la Banque interaméricaine de développement de novembre 2018 Crimen y violencia: Un obstáculo para el desarrollo de las ciudades de América Latina y el Caribe | Publications (iadb.org)
2. Selon l'ONG mexicaine « Conseil citoyen pour la Sécurité publique et la Justice pénale » dont le travail est internationalement reconnu : Boletín Ranking de las 50 ciudades más violentas del mundo 2020 (seguridadjusticiaypaz.org.mx)
3. À l'heure actuelle, il n'existe pas de statistiques fiables sur la proportion de délits et de crimes commis impliquant l'usage de nouvelles technologies mais les récentes études montrent une proportion croissante, notamment in Cybercrimes et enjeux technologiques - Contexte et perspectives – sous la direction de Francis Fortin – Presses internationales Polytechnique – 2020.
4. Capacité pour des criminels ou des groupes criminels de développer des outils, des kits, des services très spécifiques qu'ils vendent ou louent à d'autres criminels ou groupes criminels qui ne disposent pas de ces capacités spécialisées. Le crime as a service est notamment très répandu en matière de cybercrime et de blanchiment d'argent qui impliquent des connaissances spécifiques dont tous les criminels / groupes criminels ne disposent pas. C'est aussi souvent plus rapide et plus économique pour ces groupes que de développer des « compétences » internes.
5. Digital 2021: Global Overview Report — DataReportal – Global Digital Insights
6. Serious and Organized Crime Threat Assessment (SOCTA) : European Union serious and organised crime threat assessment | Europol (europa.eu) (version 2021)
7. Instrument de Documentation et d'Évaluation de la menace en Amérique Latine (IDEAL) : Documento-web-2.MB .pdf (elpaccto.eu) (document en espagnol)
8. Argentine, Chili, Colombie, Costa Rica, Panama, Paraguay, Pérou et République Dominicaine – Parties / Observateurs à la Convention de Budapest et Organisations Observateurs au T-CY (coe.int)
9. Brésil, El Salvador, Nicaragua et Uruguay.
10. STCE 185 - Convention sur la cybercriminalité (coe.int)
11. Internet Organized Crime Threat Assessment : INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020 | Europol (europa.eu)
12. Comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI) : Comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI) - Consilium (europa.eu)

LA CORRUPTION EN AFRIQUE

IHSANE EL HASSANI

PROFESSEURE HABILITÉE À LA FACULTÉ DES SCIENCES JURIDIQUES, ÉCONOMIQUES ET SOCIALES DE CASABLANCA (MAROC)

Visible à tous les niveaux de la société, la corruption fait perdre au continent africain des milliards de dollars chaque année. Ses effets sur la société et l'économie sont dévastateurs. Elle détruit sa croissance, freine son développement et dégrade le bien être de sa population.

Chaque année, 38 milliards de dollars échappe au continent à cause des transactions illégales des multinationales qui impactent le développement du continent. Selon Global Financial Integrity, les multinationales et autres établissements privés sont à l'origine de 60 à 65% des flux financiers illicites mondiaux dont la corruption représente probablement une part importante provenant des pays les moins avancés.

En 2003, les États membres de l'Union africaine y compris le Maroc ont adopté la Convention de l'Union Africaine sur la Prévention et la Lutte contre la Corruption (CUAPLC) visant à renforcer la mise en place par chacun des États parties des mécanismes nécessaires pour prévenir, détecter, réprimer et éradiquer la corruption et les infractions assimilées dans les secteurs public et privé. Également, la communauté internationale a adopté diverses conventions internationales anti-corruption notamment la Convention des Nations Unies Contre la Corruption (CNUCC) adoptée en 2003 et ratifiée par des pays africains y compris le Maroc en 2007. Cette ratification a poussé les États membres à adopter des cadres juridiques et mettre en place des institutions dédiées à la lutte contre la corruption comme l'Instance Nationale de Probité, de la Prévention et de la Lutte contre la Corruption (INPPLC) qui remplace l'Instance Centrale de prévention de la corruption créée en 2007, cas du Maroc.

Les lois anti-corruption sont-elles vraiment adoptées et appliquées par les pays africains ? Les agences anti-corruption sont-elles dotées de ressources suffisantes leur permettant d'accomplir efficacement leurs missions ? Disposent-elles de larges pouvoirs leur permettant de prévenir et lutter contre ce crime ? Élaborent et mettent-elles en application des stratégies efficaces anti-corruption ?

Frappée de plein fouet par la Covid-19, l'Afrique se trouve incapable de résister à un autre virus à l'instar de celui de la corruption. Dans beaucoup de pays, les mécanismes de lutte contre la corruption ont été suspendus et les acteurs de la corruption profitent de cette crise. Les pouvoirs publics ont adopté des mesures sociales et économiques et ont dépensé des sommes importantes afin de gérer au mieux la crise et relancer les économies. Mais, une part de ces sommes serait disparue à cause des détournements et de la corruption. Cette dernière fragilise la réponse sanitaire mondiale à la Covid-19.

L'ampleur et la gravité de ce fléau dans le monde et en particulier en

Afrique ont été bien illustrées par Transparency International (TI) dans son rapport publié en 2021 sur l'indice de perception de la corruption (IPC). En effet, seulement 6 sur 54 pays africains ont obtenu un score supérieur à 50/100. Ce qui témoigne l'omniprésence de la corruption dans le continent.

Quelles sont donc les causes expliquant ce mauvais score qui, pour certains pays, s'est vu même dégrader ? Quelles sont les initiatives lancées par les gouvernements africains pour mettre fin à cette infraction pénale pesant lourdement sur les économies du continent ? Quelles sont les politiques publiques à même d'endiguer ce crime dont souffre le continent africain depuis des années ?

Cet article se veut d'apporter des éléments de réponse à ces questions et ce, à travers les principaux axes ci-dessous : Pourquoi l'Afrique est classée parmi les continents les plus corrompus de la planète ? (I) ; Comment les multinationales favorisent-elles la corruption au sein de l'Afrique ? (II) ; Comment remédier à ce fléau qui gangrène les institutions publiques ? (III)

I. L'Afrique, l'un des continents les plus corrompus

La corruption coûte 148 milliards de dollars par an à l'Afrique. À cela s'ajoute un autre fardeau, celui de la crise sanitaire. En 2020, 41 économies africaines ont enregistré une baisse de leur PIB induite par la crise.[1]

A. C'est quoi la corruption ?

Reconnue officiellement en 1996 comme un cancer qui gangrène les circuits financiers du développement, la corruption se produit là où convergent les intérêts politiques, bureaucratiques et économiques et aboutit à l'enrichissement personnel du corrompu. Sur le plan institutionnel, la corruption plonge ses racines dans la délégation de pouvoir. Cette idée est confirmée par l'équation posée par l'économiste américain Robert Klitgaard : Corruption = monopole + pouvoir discrétionnaire - responsabilité. Pour lui la corruption se prolifère dès qu'une minorité d'individus jouisse d'une position monopolistique et dispose d'un pouvoir discrétionnaire de décision, en l'absence d'un système de responsabilisation.

Les organisations internationales telles que la Banque Mondiale (BM), l'Organisation des Nations Unies (ONU) et TI définissent la corruption d'une manière très large comme étant « l'abus du pouvoir conféré par une fonction publique à des fins d'enrichissement personnel».

Ni la CNUCC, ni la CUAPLC n'ont donné une définition précise de la corruption, mais chacune a listé toute une série de pratiques de corruption qui sont érigées en infraction par le droit pénal de plusieurs pays telles que[2] :l'abus de pouvoir, l'enrichissement illicite, le trafic d'influence, les pots de vin, les conflits d'intérêts, le blanchiment d'argent, le détournement de fonds, la fraude, l'extorsion, le népotisme, le délit de favoritisme, la distribution des faveurs, les dons illicites et les commissions, le délit d'initié, la soustraction de biens dans le secteur privé et crimes des cols blancs.

B. Les formes de la corruption

La corruption sévit dans tous les niveaux de l'administration. Elle prend des formes différentes. Publique ou privée, active ou passive voire législative lorsque les politiciens trahissent leurs électeurs en vendant leurs votes à des groupes de pression. La Banque mondiale (BM) distingue entre la petite corruption pratiquée en bas d'échelle, qui est la corruption bureaucratique dans l'administration publique, et la grande corruption à haut niveau où les décideurs politiques créant et appliquant les lois utilisent leur position officielle pour promouvoir leur bien-être et leur pouvoir personnel.

La grande corruption se trouve au coeur de la vie économique et politique de l'Afrique. Elle est nourrie pour la grande part par la corruption internationale. La Convention s'intéressant à ce type de corruption est la Convention anticorruption d'agents publics étrangers dans les transactions commerciales internationales entrée en vigueur en 1999.

C. Les actes de corruption les plus répandus en Afrique

Selon le Secrétaire général de l'ONU, la crise sanitaire engendrée par la Covid-19 ouvre la voie à de nouvelles pratiques de corruption[3]. Plus de 1800 femmes et hommes ont contacté le réseau mondial des centres d'assistance juridique et d'action citoyenne de TI pour signaler des

actes de corruption. Ci-après les principaux actes de corruption dominés en Afrique :

i. Les pots-de-vin

Répandu en Afrique, ce fléau est exacerbé avec la propagation de la Covid-19. Selon TI, 75 millions de personnes en Afrique versent des pots-de-vin. En effet, pour obtenir de meilleurs services de santé et d'éducation, certains citoyens estiment qu'il est nécessaire de payer un pot-de-vin[4]. C'est ainsi que pour accéder aux équipements de protection individuelle et tests de Covid-19, des patients ont versé des pots-de-vin et le personnel médical, vu son faible salaire, a *accepté des pots-de-vin en période de crise*[5].

ii. Le détournement de fonds

Dans certains pays africains, l'État a pu récupérer dans ses caisses des millions de dollars des salaires des fonctionnaires fictifs[6]. Cela laisse présumer des détournements d'argent dans ces pays. En période de crise, une part des fonds publics aurait été détournée sous forme de fraudes, d'achats de produits non nécessaires, d'attribution de contrats publics à des entreprises non agrées[7], de commande de masques de protection facturés hors de prix pour le pays[8] et de dons destinés aux victimes de coronavirus non distribués[9].

iii. La fraude

En Afrique, des attaques d'ingénierie sociale se sont intensifiées pendant la période de la crise y compris l'hameçonnage sous ses différentes variantes, telles que le spear phishing et le vishing, ainsi que la création de faux sites web d'entreprise pour tromper des acheteurs.

iv. Les élections truquées

Les élections libres et honnêtes demeurent rares en Afrique. Souvent, les élections débouchent sur des vagues de violence à cause de l'absence ou le non-respect des règles du bon fonctionnement du marché politique qui signifie le respect du droit de vote des électeurs et du droit d'éligibilité des candidats. Malheureusement, les listes électorales sont souvent falsifiées.

v. Le favoritisme

En période de la Covid-19, beaucoup de personnes souhaitent être vaccinées le plus vite possible. De ce fait, pour leur rendre le service rapidement, des médecins fraudent le système d'enregistrement afin de faire passer leurs proches en priorité[10].

D'autres actes de corruption peuvent s'ajouter aux pratiques de corruption susmentionnées comme les transactions douteuses avec des firmes multinationales intervenant dans le secteur des ressources naturelles et les transferts de fonds illégaux vers l'étranger et les irrégularités comptables, notamment par la dissimulation.

Après avoir énuméré les principaux actes de corruption, se pose alors la question des conséquences de cette technique de la criminalité financière.

D. Les conséquences de la corruption

La corruption a des conséquences économiques et sociales graves. Elle porte préjudice au libre-échange, décourage les investissements directs étrangers et étouffe la croissance économique. Elle détourne les dépenses publiques vers les projets qui procurent facilement les pots-de-vin, au détriment des programmes prioritaires. Elle alimente le secteur informel, encourage la fraude fiscale, la fuite de capitaux et par conséquent réduit les recettes de l'État. Elle affaiblit la crédibilité des institutions, dégrade le classement et l'image du continent au niveau international, démotive les citoyens à la participation politique, marginalise le pauvre à l'accès aux services sociaux et anéantit la confiance de la société dans les institutions publiques et les gouvernements.

La corruption est responsable de la dégradation des biens et des services publics et menace même la sécurité. Elle affaibli aussi les institutions locales d'application de la loi et de contrôle des frontières et affecte leur légitimité et leur crédibilité auprès du public et fausse le rôle redistributif de l'État et favorise la pauvreté[11]. La corruption creuse également les profondes inégalités mises à nu par la pandémie et fait obstacle à une reprise vigoureuse.

En cette période de crise, elle compromet le succès de la lutte contre la pandémie et contribue ainsi indirectement à une propagation plus rapide du virus.

E. La gravité de la corruption et son impact sur le secteur public africain

Le classement établi par TI de l'ensemble des pays africains selon l'indice de perception de la corruption (IPC) de 2013 à

2020 est retracé dans le tableau ci-dessous[12].

Le tableau montre que la situation de certains pays africains en matière de lutte contre la corruption continue de s'aggraver entre 2013- 2020. C'est le cas notamment de la Guinée, la Mauritanie, le Cameroun, la République Démocratique de Congo, le Niger, le Nigeria, l'Angola, le Mali, le Cameroun, le Tchad, la Lybie, le Soudan du Sud et la Somalie.

La mauvaise note attribuée à la majorité des pays africains est due notamment à la mauvaise gouvernance qui signifie en général le maintien d'un système judiciaire inadéquat, la mise en place des cadres juridiques et réglementaires insuffisants, le manque de transparence et de liberté de la presse. De même, les conflits ethniques et religieux, les guerres civiles frappant certains pays africains, l'exploitation illicite des ressources par des sociétés étrangères, le faible salaire des cadres, le manque de volonté politique, l'absence des sanctions dans les affaires de corruption, l'absence de mécanismes efficaces de contrôle et de reddition des comptes, la dégradation de la déontologie professionnelle, le manque de coordination entre les acteurs de la lutte anti-corruption, l'absence de stratégie nationale anti-corruption et l'insuffisance des moyens des agences anti-corruption sont autant de facteurs qui favorisent la corruption en Afrique.

Avec la propagation de la pandémie Covid-19, la corruption s'est intensifiée en Afrique. Pour TI, même les pays moins corrompus ne sont pas immunisés contre le virus de la corruption qui reste difficile à endiguer.

Certains pays africains notamment la Côte d'Ivoire, le Sénégal, la Tunisie et le Maroc ont pu réaliser des progrès dans la répression de ce crime. Bien que la plupart des pays affirment avoir mis en place de meilleurs dispositifs anti-corruption, le paradoxe est que la corruption semble être de plus en plus endémique.

Le Maroc qui en 2020, est classé à la 86ème place avec un score de 40 points dans un classement comprenant 180 pays se situe toujours

	Scores							
Pays	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Botswana	64	63	63	60	61	61	61	60
Seychelles	54	55	55	55	60	66	66	66
Cap Vert	58	57	55	59	55	57	58	58
Maurice	52	54	53	54	50	51	52	53
Rwanda	53	49	54	54	55	56	53	54
Namibie	48	49	53	52	51	53	52	51
Sénégal	41	43	44	45	45	45	45	45
Afrique du Sud	42	44	44	45	43	43	44	44
Ghana	46	48	47	43	40	41	41	43
Burkina Faso	38	38	38	42	42	41	40	40
Tunisie	41	40	58	41	42	42	43	44
Zambie	38	38	38	38	37	35	34	33
Libéria	38	37	37	37	31	32	28	28
Maroc	37	39	36	37	40	43	41	40
Gabon	34	37	34	35	32	31	31	30
Niger	34	35	34	35	33	34	32	32
Côte d'Ivoire	27	32	32	34	36	35	35	36
Ethiopie	33	33	33	34	35	34	37	38
Algérie	36	36	36	34	33	35	35	36
Egypte	32	37	36	34	32	35	35	33
Mali	28	32	35	32	31	32	29	30
Nigeria	25	27	26	28	27	27	26	25
Guinée	24	25	25	27	27	28	29	28
Mauritanie	30	30	31	27	28	27	28	29
Cameroun	25	27	27	26	25	25	25	25
RD Congo	22	22	22	21	21	21	18	18
Tchad	19	22	22	20	20	19	20	21
Angola	23	19	15	18	19	19	26	27
Libye	15	18	16	14	17	17	18	17
Soudan du Sud	14	15	15	11	12	12	12	12
Somalie	8	8	8	10	9	10	9	12

Source : Transparency International

dans une zone de corruption endémique avec un score moyen de 38,75 sur les 8 dernières années, et ce, malgré les efforts déployés pour lutter contre la corruption. Selon TI, cette note est due au manque de volonté politique quant à sa mise en oeuvre tout en citant l'exemple des tergiversations des groupes politiques au sujet du projet de loi sur l'enrichissement illicite qui a duré longtemps[13].

Le Maroc qui vise à assainir les secteurs prioritaires touchés par la corruption, améliorer son score, relever son classement et son image au niveau international a adopté une panoplie de mesures telle que la loi sur l'accès à l'information, la loi sur la déclaration du patrimoine, le numéro vert pour dénoncer la corruption, le projet de loi sur la protection des lanceurs d'alerte dans la fonction publique, la mise en place de cartographie des risques de corruption dans les ministères et la promulgation de la loi n° 46-19 adoptée le 13 mai 2021 portant création de l'INPPC. Également, le Royaume a adopté en 2007, la loi 43-05 anti-blanchiment et en 2021, la loi n° 12-18, qui a modifié et complété le Code pénal et la loi 43-05 précitée dans le but de renforcer le dispositif juridique de lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi qu'à l'adapter aux normes internationales adoptées par le Groupe d'Action Financière.

Le Royaume a déjà créé en 2017 une commission nationale anti-corruption chargée de superviser et de suivre la mise en place de la stratégie anti-corruption lancée en 2015 et a mis en place un plan national de lutte contre toutes formes de corruption à l'horizon 2025 ayant pour objectif de moraliser davantage la vie publique et renforcer la confiance des citoyens dans l'administration et les établissements publics et semi-publics. Malgré la propagation de la Covid-19, le Royaume table sur un score de 60/100 dans l'IPC en 2021.

Les pays les moins corrompus de l'Afrique sont le Botswana, le Cap Vert, l'Ile Maurice, les Seychelles, le Rwanda et la Namibie. Ils ont affiché ces huit dernières années des notes supérieures à la moyenne 50/100. Ces pays ont dû faire face à des problèmes de corruption favorisée notamment par le manque de transparence dans les dépenses publiques réalisées en réponse à la Covid-19.

De même, les gouvernements africains ont pris des mesures exceptionnelles en réponse à l'urgence sanitaire, notamment en matière de marchés publics. Au Maroc, ces mesures ont introduit des allégements spéciaux pour lesquels le gouvernement marocain n'a pas été tenu de rendre des comptes[14].

II. La corruption dans le secteur extractif

La prise en compte de la dimension transnationale de la corruption en Afrique aide à s'attaquer au problème de la corruption à la racine. La question de la corruption transfrontalière est traitée par la convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales. Le seul pays africain à avoir y adhéré est l'Afrique du Sud et ce en 2007.

A. Les actes de corruption dans les sociétés multinationales

L'Afrique est dotée d'immenses ressources minérales, gazières et pétrolières lui permettant de favoriser la croissance et le développement du continent. Les bénéfices tirés de l'exploitation de ces ressources profitent- ils vraiment à la population africaine ?

Les multinationales bénéficient d'une main d'oeuvre abondante à bas prix et des conditions fiscales avantageuses à long terme leur permettant de réaliser des chiffres d'affaires importants au détriment des États africains et de leur population. Ces sociétés profitent du vide législatif qui laisse le champ libre à l'apparition de grandes affaires de corruption en Afrique.

Les redevances minières versées aux États par ces sociétés sont détournées par une minorité laissant les populations vivre dans des situations précaires. Parfois même, les profits tirés par les multinationales des exploitations minières et pétrolières sont transférés à l'étranger sans bénéfice pour les populations locales ou ne sont pas entièrement déclarés et reversés dans les caisses des États africains[15]. Pareillement, des entreprises étrangères continuent de verser des pots-de-vin à des fonctionnaires africains pour remporter des appels d'offres, obtenir des marchés surfacturés et décrocher des contrats pétroliers. Ces

actes frauduleux coûtent chers à l'Afrique et nuisent au développement et renforcent la pauvreté du peuple africain.

Le continent perd chaque année 38 milliards de dollars dans les industries extractives[16]. Pour renflouer les caisses des différents gouvernements, la maximisation des revenus du secteur extractif demeure un outil puissant stimulant l'agriculture et le développement infrastructurel du continent africain. Quelles sont donc les mesures que doivent prendre les gouvernements africains pour optimiser les revenus du secteur extractif ?

B. Optimisation des revenus du secteur extractif

Pour optimiser les sources de revenus du secteur extractif, les gouvernements africains sont appelés à :

- Négocier les contrats de manière transparente avec les compagnies étrangères et ce par l'application des lois imposant la transparence sur les contrats. Rappelons qu'avec l'adhésion des pays africains à l'initiative pour la transparence des industries extractives[17], la plupart des pays africains ont adopté des lois imposant aussi bien la transparence sur les contrats que sur les études d'impact sur l'environnement. Mais, ces lois ne sont pas toujours appliquées dans la pratique. Souvent, les rapports publiés et les études ne sont pas accessibles à la population[18].

- Concevoir un régime fiscal optimal qui attire les investisseurs et continue à optimiser la génération de recettes pour le continent.

- Transformer leurs matières premières plutôt que de les exporter à l'état brut car cette transformation leur procure de la valeur ajoutée.

- Planifier les investissements publics tout en évaluant chaque projet. Sur ce point, le modèle du Botswana est exemplaire. Le pays a créé un fonds d'investissement public[19] créé en 1994 pour gérer au mieux les richesses minières du pays. Les excédents de revenus sont investis dans d'autres secteurs de l'économie. L'objectif de ce fonds est de préparer le pays après fin d'exploitation des ressources naturelles et d'en faire profiter les générations futures.

Pour leur part, les multinationales doivent publier tous les versements[20] faits à des gouvernements, projet par projet, dans chaque pays où elles mènent des activités d'exploitation ou d'exploration. Les revenus tirés de ces industries contribuent à l'amélioration des conditions de vie de la population et l'extraction de ces ressources doit être menée d'une manière responsable pour le bénéfice du pays et de son citoyen.

III. Endiguer la corruption : Quelques pistes de réflexion

Lutter efficacement contre la corruption et améliorer le score des pays africains exige l'application d'un certain nombre de mesures dont notamment :

- La volonté politique réelle des gouvernements à éradiquer la corruption et ce à travers, entre autres, la mise en oeuvre effective des stratégies anti-corruption axées sur des lois efficaces, un pouvoir judiciaire indépendant vis-à-vis des politiques.

- Le renforcement du cadre juridique qui doit être bien adapté et conforme aux instruments internationaux de lutte contre la corruption et ce notamment par la mise en oeuvre effective des lois anti-corruption. Rappelons que dans plusieurs pays africains, les lois portant sur la protection des dénonciateurs, les conflits d'intérêts, la déclaration du patrimoine, l'enrichissement illicite, l'accès à l'information et la loi sur le financement des partis politiques font défaut.

- La mise en oeuvre des réformes nationales visant à lutter contre les flux financiers illicites, restituer les ressources volées et renforcer la bonne gouvernance. Le maintien de celle-ci et la mise en place de solides institutions de gouvernance sont de nature à, non seulement lutter contre la corruption, mais aussi accélérer et poursuivre les efforts visant à réaliser le développement économique et social du continent. Peut-on suivre le modèle du Botswana qui, grâce à l'exploitation rationnelle de ses mines de diamant et à la bonne gouvernance de ses dirigeants a pu lutter contre ce crime[21] ?

- L'instauration de systèmes plus solides pour éradiquer

l'enrichissement illicite des fonctionnaires. L'accusé doit apporter des éléments de preuve justifiant l'origine de ses biens, faute de quoi il sera condamné et ses biens seront confisqués. Selon la CUAPLC, la répression des auteurs présumés de ce crime est souvent empêchée par l'immunité politique dont bénéficient lesdits auteurs[22].

- L'adoption d'une politique de tolérance zéro en matière de corruption sous toutes ses formes tout en adoptant une politique d'intégrité au sein des administrations publiques pour que leurs membres réagissent avec intégrité.

- Les agences anti-corruption doivent disposer de larges pouvoirs, de moyens financiers suffisants et de personnel qualifié et en nombre suffisant et ayant la possibilité de travailler de manière indépendante, sans interférence politique.

- Le partage d'expérience entre ces agences anti-corruption et la promotion de la bonne coopération institutionnelle entre elles.

- La création et le renforcement des instances de contrôle chargées de superviser les agences anticorruption regroupant le Parlement, la Justice, le secteur privé et la société civile chargée d'évaluer leur fonctionnement et de formuler des recommandations pour une plus grande efficacité.

- La mise en place d'institutions spécialisées aux compétences multiples dotées à la fois de pouvoirs préventifs et répressifs avec un large éventail d'activités qui vont au-delà des seules enquêtes pénales (l'éducation, la prévention et la sensibilisation). Le cas de la Direction de la corruption et de la criminalité économique du Botswana est un exemple à suivre.

- La mise en place d'un observatoire de suivi de la corruption dans les secteurs public et privé apte de mener des enquêtes et des recherches de terrain dans l'objectif d'analyser le phénomène et évaluer son impact. Observatoire qui doterait les agences anti-corruption d'un tableau de bord interne détaillant tous les indicateurs relatifs au phénomène tout en tenant compte des indicateurs mondiaux portant sur la prévention de la corruption.

- Le renforcement de la capacité d'action des réseaux des institutions nationales de lutte contre la corruption en Afrique en leur octroyant des moyens financiers leur permettant de promouvoir la coopération interinstitutionnelle, l'échange des expériences et des informations et contribuer ainsi au renforcement de la lutte contre la corruption.

- La promotion de la culture de l'éthique et de la déontologie dans la fonction publique ainsi que la modernisation de l'Administration, notamment par la réforme administrative. Il est jugé anormal de corrompre un fonctionnaire pour obtenir un service gratuit. Remédier à ce type de comportement consiste à simplifier les procédures administratives et développer l'administration numérique afin d'améliorer la relation et réduire le contact entre celle-ci et le citoyen.

- La nécessité de publier les données sur les dépenses et la distribution des ressources publiques notamment en situation de crise afin de garantir des réponses politiques justes et équitables. De même, les gouvernements devraient veiller à ce que les citoyens reçoivent de manière compréhensible, opportune et significative les informations en garantissant leur droit d'accès à l'information.

- La transparence dans la passation des marchés publics afin de lutter contre les malversations et garantir une tarification équitable. En effet, en période de confinement, de nombreux pays y compris le Maroc ont adopté une panoplie de mesures visant à assouplir les procédures des marchés publics. Mais, ces assouplissements risquent de favoriser la corruption et le détournement des ressources publiques.

- La protection des lanceurs d'alerte. Ces derniers apportent souvent des preuves déterminantes permettant de faire aboutir avec succès les poursuites engagées.

- La lutte contre la corruption passive qui nourrit les élections truquées et la mise en place de la loi régissant le financement des partis politiques pour diminuer les risques de corruption.

- La sensibilisation de la population aux pratiques de corruption, à la démocratie et l'amélioration de l'éducation par l'intermédiaire de l'école

et des médias. Ces derniers et la société civile doivent pouvoir fonctionner sans ingérence ou intimidation.

- Le renforcement des formations pour les enquêteurs, les analystes et les magistrats.

- La lutte contre l'impunité avec la condamnation de personnes pour des faits de corruption.

- L'adhésion à la convention de l'OCDE contre la corruption transnationale. Elle fait obligation aux parties de confisquer les pots-de-vin et les éventuels profits qui en découlent.

- L'application par les chefs d'entreprises et les conseils d'administration des entreprises, y compris les multinationales opérant en Afrique, des normes internationales les plus strictes en matière de lutte contre la corruption et le blanchiment de capitaux.

- L'achèvement par certains États africains de l'ensemble du processus de ratification de la CUAPLC. Selon TI, les pays qui ont ratifié ladite Convention doivent finaliser et soumettre des rapports d'avancement au conseil consultatif de l'Union Africaine (UA) sur la corruption dès que possible[23]. L'UA doit rendre tous les rapports d'avancement accessibles au public afin que les citoyens puissent suivre les engagements internationaux de leurs gouvernements en matière de lutte contre la corruption.

- Enfin, les gouvernements africains, entreprises, société civile et autres parties prenantes doivent, dans la phase post crise, réaffirmer leur détermination à travailler de concert pour renforcer la surveillance, la responsabilité, la transparence et mettre fin à toutes formes de corruption pour un continent plus prospère et équitable.

Notes :

1. Groupe de la Banque Africaine, «_Lutte contre la corruption en Afrique : la Banque africaine de développement et l'OCDE appellent à plus de vigilance dans le contexte actuel de crise sanitaire », 15 avril 2021.
2. Nations Unies, Commission économique pour l'Afrique, Rapport sur la gouvernance en Afrique IV « Mesurer la corruption en Afrique : prendre en compte la dimension internationale », 2016.
3. Nations Unies, « Journée internationale de lutte contre la corruption », 09 décembre 2020.
4. Transparency International «Comment la corruption rend les gens malade», 14 septembre 2020. `
5. Actualités/Afriques, «Covid-19, le virus de la corruption», 31 juillet 2020.
6. Sputnik France, «En Tanzanie, 10 000 âmes mortes touchaient leurs salaires», le 17 mai 2016.
7. Le point Afrique « Fonds anti- Covid : 17 millions de dollars détournés en Afrique du Sud », 06 février 2021.
8. Actualités/Afrique, « Six mois de pandémie de Covid-19 et six mois de corruption» , 11 septembre 2020.
9. Le point, « Manaouda Malachie a-t- il détourné 4000 Sacs de Riz d'Orca ? », 23 juillet 2020.
10. Courrier international « Triche. En Afrique du Sud, les fraudeurs aux vaccins dans le viseur », 15 mars 2021.
11. Nations Unies, Commission économique pour l'Afrique, Rapport sur la gouvernance en Afrique IV, « Mesurer la corruption en Afrique : prendre en compte la dimension internationale », 2016.
12. Rapports de Transparency International: de 2013 à 2020.
13. TELQUEL, « Lutte anti-corruption : Le Maroc toujours aussi mauvais élève », 29 janvier 2021.
14. Les Eco.ma, « Corruption : La Covid-19 a compliqué la donne », 03 février 2021
15. Libération, « Comment les multinationales escroquent l'Afrique ? », 02 juin 2015.
16. Le 360 Afrique. Com, «Industries extractives : L'Afrique perd 38 milliards de dollars par an dans les transactions illégales», 01 juin 2017.
17. Lancée en 2003 par Tony BLAIR, l'ITIE est une norme mondiale qui vise à promouvoir une gestion ouverte et responsable des ressources du secteur extractif. Son objectif est de rendre public et rapprocher les versements effectués par les industries extractives et les encaissements réalisés par l'État (taxes, redevances et bonus de signature). De même promouvoir et renforcer l'approche axée sur le dialogue entre une multiplicité de parties prenantes.
18. Jeune Afrique, « Industries extractives : La transparence protège (aussi) le business en Afrique », 14 février 2021.
19. Le Quotidien, «La hollande ou la RDC, la Norvège ou le Botswana ? », 08 mai 2017.
20. « OPEN DATA, l'exemple des industries extractives », décembre 2016.
21. Nations Unies Commission économique pour l'Afrique, « le Botswana suscite une lueur d'espoir dans la lutte contre la corruption en Afrique », 18 juin 2018.
22. Transparency International, « Les pays africains luttent-ils contre la corruption et poursuivent-ils des crimes qui en découlent ? », 04 février 2021.
23. Transparency International, « Le sommet de l'Union Africaine doit être l'occasion de respecter les engagements de la convention de lutte contre la corruption », 02 février 2021.